Alarm Control Panels

INTEGRA

Firmware version 1.13

USER MANUAL

SATEL sp. z o.o.
ul. Budowlanych 66
80-298 Gdańsk
POLAND
tel. + 48 58 320 94 00
info@satel.pl
www.satel.eu

integra_u_en 10/14

WARNING

Before you start using the control panel, please read carefully this manual in order to avoid mistakes that can lead to malfunction or even damage to the equipment.

Changes, modifications or repairs not authorized by the manufacturer shall void your rights under the warranty.

The INTEGRA control panels should only be connected to the **analog subscriber lines**. In case of changing the analog line to the digital one, it is necessary to contact the alarm system installer.

Pay special attention if the telephone line used by the control panel is frequently busy and/or failures are reported, concerning the line and/or monitoring. Report such situations to the alarm system installer immediately.

To ensure adequate protection, the alarm security system must be in good working order, therefore SATEL recommends that it be regularly tested. The control panel is equipped with a number of self-diagnostic functions which, when properly configured by the installer, ensure control over correct functioning of the system.

The alarm security system cannot prevent burglary, assault or fire from happening, but it guarantees that in case of emergency measures will be taken to reduce the possible damage (the alarm will be signaled optically and acoustically, appropriate services will be notified, etc.), which may deter the potential burglars.

The SATEL's goal is to continually upgrade the quality of its products, which may result in alterations of their technical specifications and firmware. The current information on the introduced modifications is available on our website.
Please visit us at:
http://www.satel.eu

The declaration of conformity may be consulted at www.satel.eu/ce

Factory default codes:

Service code: 12345

Object 1 master user (administrator) code: 1111

The following symbols may be used in this manual:

- note;
- caution.

Changes made to the firmware version 1.13

User menu	Support for the user menu shortcuts can be disabled by the installer. For some functions, when editing the multiple-selection lists in text mode, you can press the key 0 and enter the number of element (e.g. zone, partition) to be edited.

CONTENTS

1. General 4
2. Technical reliability of the alarm system 4
3. Alarm system operating costs 4
4. Authorization of users 5
4.1 Authorization with two identifiers 5
4.2 Factory default codes 5
4.3 Operation under duress 6
5. Operating the alarm system by means of LCD keypad 6
5.1 Keypads description 6
5.1.1 LCD display 6
5.1.2 LED indicators 8
5.1.3 Keys 9
5.1.4 Built-in proximity card reader 9
5.1.5 Sound signaling 9
5.2 [Code]# – arming / disarming menu 10
5.2.1 Arming menu 11
5.2.2 Disarming menu 11
5.3 [Code]* – user menu 11
5.3.1 Functions list 11
5.3.2 Starting functions 15
5.3.3 Menu shortcuts 15
5.3.4 Entering data by means of the LCD keypad 16
5.3.5 Description of user functions 18
5.4 Arming 23
5.4.1 Full arming without partition selection 23
5.4.2 Full arming the selected partitions 23
5.4.3 Arming in the selected mode 24
5.4.4 Quick arming 24
5.4.5 Denial of arming 24
5.4.6 Failure of arming procedure 25
5.4.7 Shortening the exit delay time 25
5.5 Disarming and alarm clearing 25
5.5.1 Alarm clearing without disarming 25
5.6 Two-code arming / disarming 25
5.7 Triggering the alarm from keypad 25
5.8 Users 26
5.8.1 User types 27
5.8.2 Adding new user 28
5.8.3 Edit user 28
5.8.4 Removing a user 29
5.8.5 Adding proximity card / DALLAS iButton 29
5.8.6 Adding keyfob 29
5.8.7 Removing keyfob 30
5.9 Master users (administrators) 31
5.10 Zone bypassing 31
5.10.1 Zone inhibiting 31
5.10.2 Zone isolating 32
5.10.3 Unbypassing 32
5.11 Viewing the event log 32

5.11.1 Viewing all events ... 32
5.11.2 Viewing the events required for Grade 2 ... 33
5.11.3 Viewing the selected events ... 33
5.11.4 Way of presenting events ... 33
5.12 Programming the partition timer ... 34
5.13 Zone testing ... 34
5.14 Outputs control ... 35
5.14.1 Controlling the MONO SWITCH type of output ... 36
5.14.2 Controlling the BI SWITCH type of output ... 36
5.14.3 Controlling the REMOTE SWITCH type of outputs ... 36
5.14.4 Controlling the roller shutter outputs ... 36
6. Using the partition keypad ... 37
6.1 Description of partition keypads ... 37
6.1.1 LED indicators ... 37
6.1.2 Keys ... 38
6.1.3 Built-in proximity card reader ... 38
6.1.4 Sound signaling ... 38
6.2 Functions available from the partition keypad ... 39
6.2.1 [Code]* ... 39
6.2.2 [Code]# ... 39
6.2.3 Quick arming ... 39
6.2.4 Triggering the alarm from keypad ... 40
6.2.5 Silencing the alarm sound at the keypad ... 40
6.2.6 Code changing ... 40
7. Using the entry keypad ... 40
7.1 LED indicators ... 40
7.2 Sound signaling ... 40
7.3 Functions available from the entry keypad ... 41
8. Using the code lock ... 41
8.1 Description of code locks ... 41
8.1.1 LED indicators ... 42
8.1.2 Keys ... 42
8.1.3 Sound signaling ... 42
8.2 Functions available from code lock ... 42
9. Confirming voice messaging ... 43
10. Call answering and telephone control ... 43
10.1 Answering phone calls ... 43
10.2 Telephone control ... 44
10.3 Audio alarm verification ... 44
11. SMS control only INTEGRA 128-WRL ... 45
12. Operating the alarm system by means of keyfob ... 45
13. Manual update history ... 47
14. Brief description of operating the system from keypad ... 50

1. General

Thank you for choosing the product offered by the SATEL Company. Wishing you full satisfaction with the choice you made, we are always ready to provide you with professional assistance and information on our products.

The SATEL Company is manufacturer of a broad range of devices dedicated for use in security alarm systems. Further information is available on our website **www.satel.eu** or at the points of sale offering our products.

2. Technical reliability of the alarm system

The alarm system is built of technical devices, the performance of which has crucial effect on the effectiveness of the facility protection. Components of the alarm system may be exposed to various external factors, such as weather conditions (e.g. outdoor sirens and, during a storm, also other devices, as a result of atmospheric discharge which may cause harm to electrical and telephone installations) or mechanical damage. Only a routine check of the system operation makes it possible to maintain a high level of burglary protection.

The control panel is provided with a number of safeguards and automatic diagnostic features to test the system performance. Detection of irregularities is signaled by the ⚠ LED on the keypad. **You should immediately respond to such a signal, and, if necessary, consult the installer**.

It is necessary to periodically carry out a functional test of the alarm system. Check that the control panel responds to violation of individual detectors, that their coverage areas are not obstructed, that there is a reaction to opening protected windows, and that sirens and telephone messaging work normally.

Detailed instructions on the system testing should be provided by the installer. It is recommended that the installer carry out periodic maintenance of the alarm system, when ordered by the user.

It is in the user's interest to foresee and prearrange the procedures to be followed when the control panel signals an alarm condition. It is important to know how to verify the alarm and identify its source on the basis of keypad information, and take appropriate measures, e.g., to organize evacuation.

3. Alarm system operating costs

The control panel can inform the users and the monitoring station about the status of protected facility. Realization of these functions by means of the phone line or GSM means financial costs. The amount of the costs incurred depends on the amount of information sent. A failure of telephone links, as well as an incorrect programming of the control panel, may result in increased costs (due to making of excessive number of calls).

Please inform the installer, which is a priority: to deliver information at any cost, or to prevent excessive costs. For example, after an event code has failed to be sent successfully to the monitoring station, the control panel may repeat attempts every few minutes to send the code or to cease the attempts to send the code until a next event occurs.

4. Authorization of users

Operation of the alarm system is possible after the user authorization, which allows the control panel to verify that the user is authorized to perform the given operation. The authorization can be done on the basis of:

- code,
- proximity card (125 kHz passive transponder, which can be in the form of card, tag, etc.),
- DALLAS iButton (chip),
- keyfob.

You can not assign the same identifier (code, proximity card, DALLAS iButton or keyfob) to two users.

For safety reasons, different people should not use the same identifier.

The installer can configure the panel so that it will not accept codes that contain less than three digits (e.g. 1111 or 1212) or consist of consecutive digits (3456).

The installer may permit the use of certain functions without the need for user authorization.

Using an invalid code, proximity card or DALLAS iButton three times may:

- *trigger an alarm;*
- *block the keypad / reader for 90 seconds.*

4.1 Authorization with two identifiers

The INT-KLCDR and INT-KLFR keypads and the INT-SCR multifunction keypads have a built-in proximity card reader. The installer can configure these devices so that the user has to use two identifiers for authorization: the code and the card. The function to be executed after the authorization depends on the second identifier:

- code – whether it will be confirmed by using the # key or the * key;
- card – whether it will be presented only or held.

4.2 Factory default codes

By default, the following codes are preprogrammed in the control panel:

service code: 12345

object 1 master user (administrator) code: 1111

The factory default codes make it possible to assign individual codes to consecutive persons who are to use the alarm system (see: section USERS p. 26).

The factory default codes should be changed as soon as possible using the CHANGE OWN CODE function available in the user menu.

The control panel can inform the user that the code change is necessary, if the code is known to other users.

The master code should not be used on a daily basis because of the risk of its being captured. It is recommended that the administrator enter for himself an ordinary user's code.

4.3 Operation under duress

When acting under duress, the DURESS type code must be used instead of the normal user code (see section USER TYPES p. 27).

5. Operating the alarm system by means of LCD keypad

SATEL offers the following keypads for INTEGRA control panels:

INT-TSG – touchscreen keypad;

INT-TSI – touchscreen keypad;

INT-KSG – LCD keypad with touch keys;

INT-KLCD – LCD keypad with mechanical keys;

INT-KLCDR – LCD keypad with mechanical keys and built-in proximity card reader;

INT-KLCDK – LCD keypad with mechanical keys;

INT-KLCDL – LCD keypad with mechanical keys;

INT-KLCDS – LCD keypad with mechanical keys;

INT-KLFR – LCD keypad with mechanical keys and built-in proximity card reader.

The keypads are available in a variety of color options for the enclosure, display and key backlight. The color variant is indicated by the additional designation in the keypad name (e.g. INT-KLCD-GR – green display and key backlight; INT-KLCD-BL – blue display and key backlight).

5.1 Keypads description

The INT-TSG, INT-TSI and INT-KSG keypads are described in separate manuals, which are delivered with these keypads.

5.1.1 LCD display

The display facilitates communication between the user and the alarm system, clearly indicating the system status. The functions available to the user are presented on the display. The display backlight can be used, if needed.

In **standby mode**, the display shows:

- in the upper line – the date and time in the format defined by the installer,
- in the lower line – the keypad name or state (status) of selected partitions (to be defined by the installer).

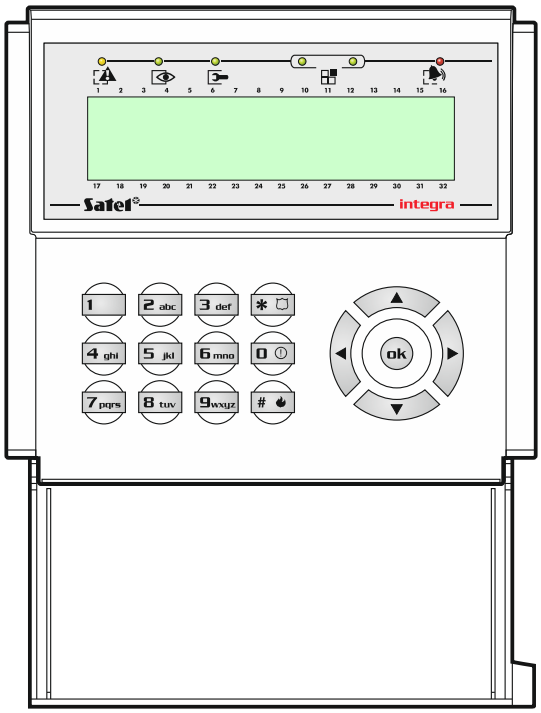
The installer can configure the keypad so that when you press the 9 key for approx. 3 seconds, the display will enter the **partition state presentation mode**. The status of partitions operated by the keypad (including those from which alarm is signaled on the keypad) is presented by means of symbols. The display will return to the standby mode after you press the 9 key for approx. 3 seconds again.

If some predefined events occur, additional messages may appear on the display (e.g. arming, disarming, auto-arm delay countdown, entry/exit delay countdown, alarm, etc.).

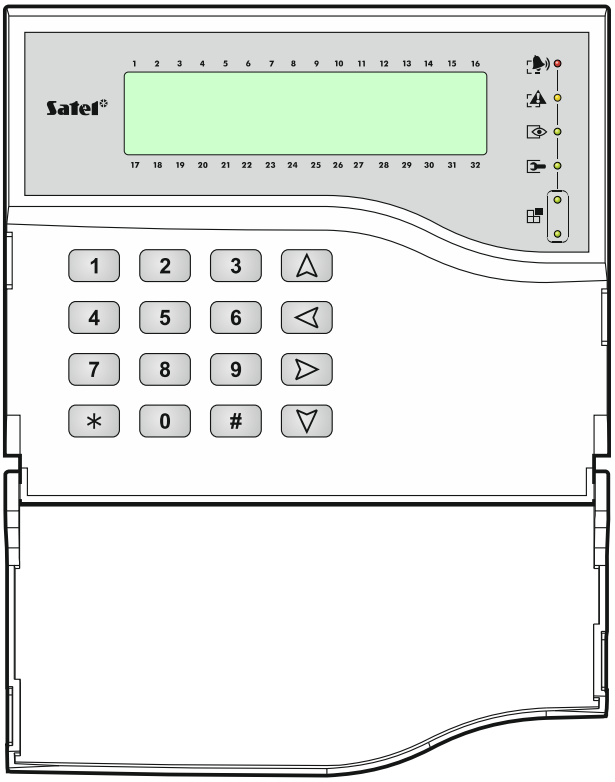
Entering the user code, i.e. the user authorization, will open a menu containing the functions that are available to the user. The functions are presented in two lines. The currently selected function is indicated by the arrow on the left-hand side. How the function related information is presented depends on the specific character of the given function.

The way of display backlighting is programmed by the installer.

INT-KLCD / INT-KLCDR



INT-KLCDK



INT-KLFR

Fig. 1. Keypads with flap.

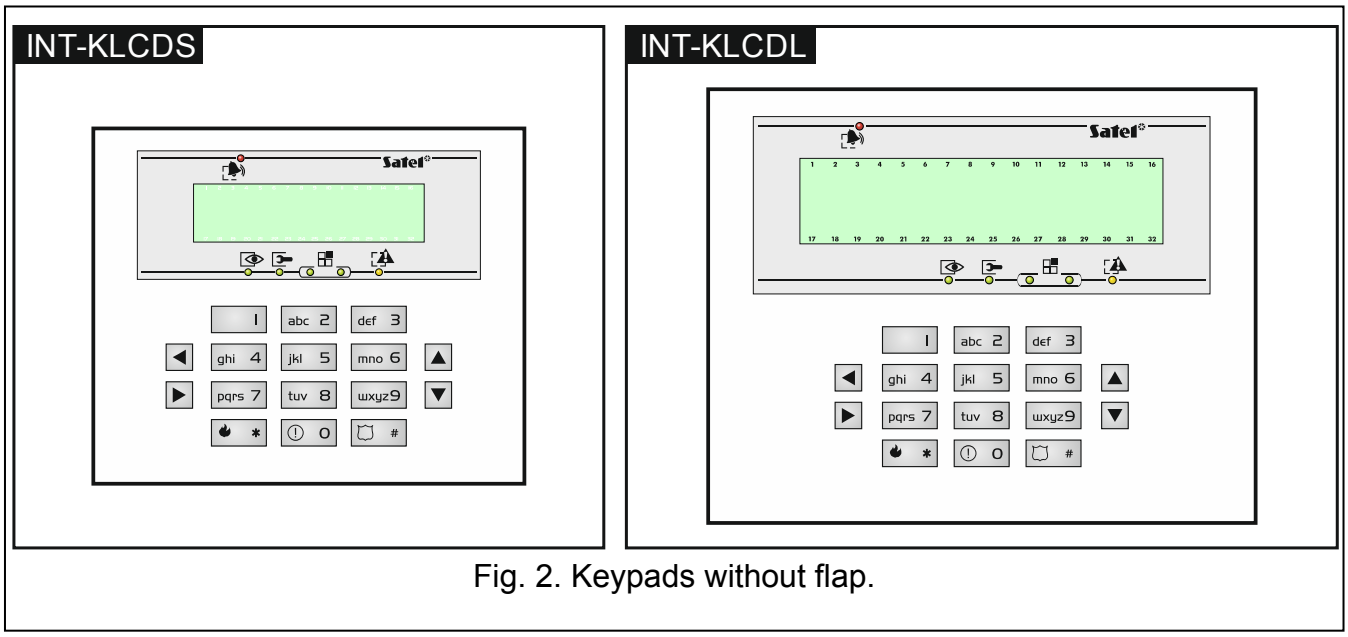


Fig. 2. Keypads without flap.

5.1.2 LED indicators

LED	Color	Function description
	green	**ON** – all keypad operated partitions are armed **blinking** – some keypad operated partitions are armed or exit delay countdown is running
	red	**ON** or **blinking** – alarm or alarm memory
	yellow	**blinking** – trouble or trouble memory
	green	**blinking** – service mode is entered
	green	if zone status is being presented or the keypad is switched to graphic programming mode (see: section SELECTION FROM THE MULTIPLE-CHOICE LIST p. 16), two LEDs indicate which data set is being displayed (see: table 2)

Table 1. Description of keypad LEDs.

Data type	LED		Information
	left side/upper	right side/lower	
Zones/Outputs	OFF	OFF	numbers 1-32
	OFF	ON	numbers 33-64
	ON	OFF	numbers 65-96
	ON	ON	numbers 97-128
Expanders	OFF	OFF	system addresses 0-31 (00-1F HEX)
	OFF	ON	system addresses 32-63 (20-3F HEX)

Table 2. Information presented by the LEDs.

Information about the armed state can be extinguished after a time period defined by the installer.

If the installer has enabled the GRADE 2 option:

- *the LEDs provide information about alarms only after the code has been entered and confirmed with the * key;*

– *blinking of the ⚠ LED means that there is a trouble in the system, some zones are bypassed, or that there was an alarm.*

5.1.3 Keys

The keys designated with digits and letters enable entering the code and data, when using the functions available in the menu. Additionally, if you press and hold down the selected digit keys for approx. 3 seconds, you can (if the keypad has been so configured by the installer):

1 - check the state of zones;

4 - check the state of partitions;

5 - view the alarm log;

6 - view the trouble log;

7 - view the current troubles;

8 - enable/disable chime signal in the keypad;

9 - toggle the display between the standby mode and partition state display mode.

The other keys enable you to:

✱ - enter the user menu (after entering the code);
- cancel the started operation.

or ok - arm / disarm and clear alarm (after entering the code);
- start the selected function;
- confirm the entered data.

◄ ▲ ▼ ► - navigate through the display (scroll through the displayed messages, functions and options, and move the cursor);
- run the installer selected functions (after entering the code).

🔥 - trigger the fire alarm.

Ⓘ - trigger the medical (auxiliary) alarm.

⛨ - trigger the panic alarm.

5.1.4 Built-in proximity card reader

The INT-KLCDR and INT-KLFR keypads can be operated by means of proximity cards (proximity tags or other 125 kHz passive transponders). The installer defines which functions can be executed after presenting or holding the card.

5.1.5 Sound signaling

Beeps generated when operating

The installer can disable the sound signaling.

1 short beep – pressing any number key.

2 short beeps – confirmation of command execution, signaling of entering the user menu, submenu or function.

3 short beeps – signaling of:

– starting the procedure of arming (there is exit delay in the partition) or arming (there is no exit delay in the partition);

– disarming and/or alarm clearing;

– turning output off;

- disabling chime signal in the keypad, using the 8 key;
- toggling the display between the standby mode and the partition status presentation mode, using the 9 key;
- exiting the function and returning to the menu after confirmation of the data entered.

4 short beeps and 1 long beep – signaling of:

- turning output on;
- enabling chime signal in the keypad, using the 8 key;
- ending the function and exiting the user menu after confirmation of the data entered.

1 long beep – signaling of:

- violated/ bypassed zones when arming;
- fault of the vibration detector (10. 24H VIBRATION type zone was not violated during the vibration detector test run upon starting the arming procedure).

2 long beeps – invalid code/card, function not available or exiting the function without confirmation of the data entered (e.g. by using the ✻ key).

3 long beeps – unavailable function.

Events signaled by sounds

Only installer selected events are signaled.

Alarms are being signaled throughout the time programmed by the installer.

5 short beeps – zone violation (CHIME).

Long beep every 3 seconds, followed by a series of short beeps for 10 seconds and 1 long beep – countdown of exit delay (if the time is shorter than 10 seconds, only the final sequence of short beeps will be generated).

A sequence of 7 beeps of diminishing duration, repeated every few seconds – countdown of auto-arming delay.

2 short beeps every seconds – countdown of entry delay.

2 short beeps every 3 seconds – signaling a new trouble.

Continuous beep – alarm.

Long beep every second – fire alarm.

5.2 [Code]# – arming / disarming menu

Information given in the section below do not apply to users having the SIMPLE USER right (see p. 27).

After you enter the code and confirm it with the # key:

- a message on the need to change the code or a service note may be displayed;
- alarm will be cleared – if the user is authorized to clear the alarm and there is an alarm in the system;
- one partition will be disarmed – if the user is authorized to disarm the partition, has access to only one partition operated from the keypad and that partition is armed, or has access to many partitions, but only one partition is armed;
- one partition will be armed – if the user is authorized to arm the partition, has access to only one partition operated from the keypad and that partition is disarmed;
- the arming/disarming menu will be displayed.

5.2.1 Arming menu

The arming menu will be displayed if:

- the user is authorized to arm the partition;
- the user has access to a number of partitions operated from the keypad;
- none of the partitions accessible to the user is armed;
- there is no alarm.

Two functions are available in the menu:

Arm all	*arming all partitions*
Arm selected	*arming selected partitions*

5.2.2 Disarming menu

The disarming menu will be displayed if:

- the user is authorized to disarm the partition;
- the user has access to a number of partitions operated from the keypad;
- at least two partitions accessible to the user are armed.

Two functions are available in the menu:

Disarm all	*disarming all partitions*
Disarm selected	*disarming selected partitions*

5.3 [Code]✻ – user menu

After you enter the code and confirm using the ✻ key, the user menu will be displayed. The list of available functions depends on the user authority level, as well as the system status and configuration. In order to exit the user menu, press the ✻ key. The keypad will quit the menu automatically, if 2 minutes have elapsed since the last keypress.

Upon entering the code and confirming with the ✻ key, a message about the need to change the code or a service note may be displayed.

5.3.1 Functions list

The functions available after entering the service code have been highlighted with white text against black background. Highlighted with a frame are functions available to the administrators.

View clear. al.	*view cleared alarms from selected partition zones*
System reset	*restore system after verified alarm*
Disarm	*disarm selected partitions*
Clear alarm	*clear alarm*
Clear other al.	*clear alarm in other objects*
Abort voice m.	*cancel telephone messaging*
Arm	*arm selected partitions*
Arm (2 codes)	*start two code arming*
Disarm (2codes)	*start two code disarming*
Defer auto-arm	*postpone the auto-arming*
Set auto-arm d.	*set auto-arming postpone time*
Arming mode	*select arming mode*
Cancel 1st code	*cancel consent to two code arming/disarming*

Change own code — *change own code*
Change tel.code — *change own telephone code*
Change prefix
- Prefix normal — *set normally used prefix*
- Prefix duress — *set duress prefix*
- Recall time — *set time to remind of the need to change prefix*

Users
- **New user** — *add new user*
  - Code — *set code*
  - Telephone code — *set telephone code*
  - Partitions — *assign partitions available to the user*
  - Type — *select type of code*
  - Schedule — *select time schedule*
  - Existence time — *set code validity time*
  - Bypass time — *set bypass time*
  - Rights — *assign rights*
  - Keypads etc. — *assign modules available to the user*
  - New prox. card — *add proximity card*
  - Rem. prox. card — *remove proximity card*
  - New DALLAS — *add DALLAS iButton*
  - Remove DALLAS — *remove DALLAS iButton*
  - New RX key fob — *add 433 MHz keyfob*
  - Rem. RX key fob — *remove 433 MHz keyfob*
  - Button 1 — *assign function to keyfob button 1*
  - Button 2 — *assign function to keyfob button 2*
  - Button 3 — *assign function to keyfob button 3*
  - Button 4 — *assign function to keyfob button 4*
  - Button 1 and 2 — *assign function to combination of keyfob buttons 1 & 2*
  - Button 1 and 3 — *assign function to combination of keyfob buttons 1 & 3*
  - Events (RX) — *set event generating rules*
  - New ABAX keyfob — *add keyfob supported by ABAX system*
  - Rem.ABAX keyfob — *remove keyfob supported by ABAX system*
  - Button 1 — *assign function to keyfob button 1*
  - Button 2 — *assign function to keyfob button 2*
  - Button 3 — *assign function to keyfob button 3*
  - Button 4 — *assign function to keyfob button 4*
  - Button 5 — *assign function to keyfob button 5*
  - Button 1 and 5 — *assign function to combination of keyfob buttons 1 & 5*
  - Events (ABAX) — *set event generating rules*
  - Confirm. (ABAX) — *set confirmation rules*
  - Name — *program user name*
- **Edit user** — *edit existing user*
  - [select user]
    - [list of parameters identical as in case of a new user]

- **Remove user** — *remove user*

Masters

- **New master** — *add new master*
  - Code — *set code*
  - Rights — *assign rights*
  - Keypads etc. — *assign modules available to the master*
  - New prox. card — *add proximity card*
  - Rem. prox. card — *remove proximity card*
  - New DALLAS — *add DALLAS iButton*
  - Remove DALLAS — *remove DALLAS iButton*
  - New RX keyfob — *add 433 MHz keyfob*
  - Rem. RX keyfob — *remove 433 MHz keyfob*
  - Button 1 — *assign function to keyfob button 1*
  - Button 2 — *assign function to keyfob button 2*
  - Button 3 — *assign function to keyfob button 3*
  - Button 4 — *assign function to keyfob button 4*
  - Button 1 and 2 — *assign function to combination of keyfob buttons 1 & 2*
  - Button 1 and 3 — *assign function to combination of keyfob buttons 1 & 3*
  - Events (RX) — *set event generating rules*
  - New ABAX keyfob — *add keyfob supported by ABAX system*
  - Rem.ABAX keyfob — *remove keyfob supported by ABAX system*
  - Button 1 — *assign function to keyfob button 1*
  - Button 2 — *assign function to keyfob button 2*
  - Button 3 — *assign function to keyfob button 3*
  - Button 4 — *assign function to keyfob button 4*
  - Button 5 — *assign function to keyfob button 5*
  - Button 1 and 5 — *assign function to combination of keyfob buttons 1 & 5*
  - Events (ABAX) — *set event generating rules*
  - Confirm. (ABAX) — *set confirmation rules*
  - Name — *set master name*
- **Edit master** — *edit existing master*
  - [select master]
    - [list of parameters identical as in case of a new master]
- **Remove master** — *remove master*

Zone bypasses

- Inhibit — *temporary zone bypass*
- Isolate — *permanent zone bypass*

Set time — *set control panel clock*

System state — *check troubles / check system state*

Events

- **Selected**
  - Select events — *select type of events to be viewed*
  - Select part. — *select partitions from which events are to be viewed*
  - View — *view selected events*

- View Grade2 — *view events required for Grade 2*
- All — *view all events*
- Grade2 — *view events required for Grade 2*

Reset zones — *reset 43. RESETABLE POWER SUPPLY type outputs*

Clr.latch.outs — *clear latched outputs*

Fin.f.door open — *end door fire opening*

Change options

- Keypad chime — *enable/disable CHIME in keypad*
- Outputs chime — *block zone violation signal. on 11. CHIME type outputs*
- Timers — *edit timers*
- Part. timers — *program partition timers*
- No exp.tamp.al. — *block expander tampers*
- Perm.serv.accs. — *enable/disable permanent installer access*
- Serv. can edit — *make user editing available to installer*
- Serv. ArmDis... — *make system control available to installer*
- Perm.DloadX acc — *enable/disable permanent DLOADX access*
- DloadX IP — *set address of computer with DLOADX program*
- GuardX IP — *set address of computer with GUARDX program*
- Erase s.message — *erase service note*

Tests

- Partitions — *check current state of partitions*
- Zones — *check current state of zones*
- Supply voltages — *check module supply voltage*
- Radio devices — *check radio signal level for wireless devices*
- Temperatures — *check temperatures measured by ATD-100 detectors*
- **Zones test**
  - **New**
    - Burglary zones — *start new test for burglary zones*
    - Fire/tech.zones — *start new test for fire and technical zones*
  - View results — *view test results*
  - Finish test — *abort test*
  - Clear results — *clear test results*
- Battery test — *test battery and 60. TECHN. - BATTERY LOW zones*
- Manual tr. test — *start manual test transmission*
- Station 1A test — *start test transmission to station 1 – main phone number*
- Station 1B test — *start test transmission to station 1 – backup phone number*
- Station 2A test — *start test transmission to station 2 – main phone number*
- Station 2B test — *start test transmission to station 2 – backup phone number*
- GPRS monit.test — *send test transmission via GPRS [only INTEGRA 128-WRL]*
- Messaging test — *start messaging test*
- Answering test — *display information on answered tel. call*
- Prox. card test — *check proximity card number*
- CA-64 PTSA test — *start mimic board test*
- View masters — *view master users*

Keypad name	*display keypad name*
File in DloadX	*display inf. on DLOADX program file with control panel data*
Panel version	*display information on control panel firmware version*
STM prg.version	*display inf. on ABAX syst. firmware [only INTEGRA 128-WRL]*
GSM IMEI/v/sig.	*display information on GSM telephone [only INTEGRA 128-WRL]*
IP/MAC ETHM-1	*disp. inf. on ETHM-1 / ETHM-1 Plus module IP and MAC address*
Modules version	*display information on module firmware version*
Time synchron.	*start time synchronization*
Service access	*set installer access time*
Open door	*open selected door controlled by system*
Outs control	*control outputs*
Service mode	*start service mode*
Take SM over	*take over service mode*
Downloading	
Start DWNL-RS	*start local programming*
Finish DWNL-RS	*finish local programming*
Start DWNL-MOD.	*start communication via external modem*
Start DWNL-TEL	*start communication via 300 bps modem*
Start DWNL-CSD	*start CSD communication [only INTEGRA 128-WRL]*
Start DWNL-GPRS	*start GPRS communication [only INTEGRA 128-WRL]*
ETHM-1 – DloadX	*start communication via Ethernet with DLOADX program*
ETHM-1 – GuardX	*start communication via Ethernet with GUARDX program*

5.3.2 Starting functions

1. Using the ▼ and ▲ keys, find the required submenu or function. The currently selected submenu or function is indicated by the arrow (➢) on the left-hand side.
2. Press the ▶ or # key to enter the submenu (the ◀ key allows to exit the submenu) or start the function.

5.3.3 Menu shortcuts

Support for the user menu shortcuts can be disabled by the installer.

You can use shortcuts for quick access to some menu elements (submenus, functions). Press the suitable digit key (or combination of keys) to enter a submenu or start a function. Shown below is the list of submenus and functions available by using shortcuts. The shortcuts are shown in square brackets.

[1] Change own code

[2] Users

- [21] New user
- [22] Edit user
- [23] Remove user

If the installer is not authorized to edit the users, the shortcuts beginning with the digit 2 will allow the installer to start the function from the MASTERS submenu.

[4] Zone bypasses

- [41] Inhibit

[42] Isolate

[5] Events

[51] Selected events

[52] All events

[6] Set time

[7] System state

[8] Outputs control

[9] Service mode

[0] Downloading

[01] Start DWNL-RS

[02] Finish DWNL-RS

[03] Start DWNL-MOD.

[04] Start DWNL-TEL

[05] Start DWNL-CSD [only INTEGRA 128-WRL]

[06] Start DWNL-GPRS [only INTEGRA 128-WRL]

[07] ETHM-1 – DloadX

[08] ETHM-1 – GuardX

5.3.4 Entering data by means of the LCD keypad

Data are saved to the control panel if you press the # key (in some keypads, the OK key is also available, whose function is exactly the same). The * key enables exiting the function without saving any changes.

Described below are general rules for entering data, however they may be different as regards some functions.

Selection from the single-choice list

Shown in the upper line of display is description of the function, and in the lower one – the currently selected item. You can scroll through the list of items, using the direction keys: ▼ (down) and ▲ (up). The ▶ and ◀ keys are not used.

Selection from the multiple-choice list

The functions that allow you to make multiple choice can be identified by an additional symbol situated at the right-hand side of the display:

– displayed item is selected / option is enabled;

· – displayed item is not selected / option is disabled.

Pressing any digit key (for some functions, this does not work with the key 0) will change the currently displayed symbol to the other one. To scroll through the list of items, use the ▼ key (down) or the ▲ key (up). For some functions, pressing the key 0 will allow you to enter the number of item to be edited (e.g. number of zone to be bypassed / unbypassed). This will speed up search.

For some functions, pressing the ▶ or ◀ key will switch the keypad into the **graphic programming mode**. The and · symbols are used to present on the display the current status of up to 32 items available in the given function (these can be e.g. zones, outputs, timers, etc.). Additionally, in case of zone bypassing, the symbol is used. The ▶ key moves the cursor to the right, and the ◀ key to the left. If the list of items is longer than 32, pressing the ▶ key when the cursor is placed over the last item will display the next list, and pressing the ◀ key when the cursor is placed over the first item will display the previous list (see also

description of the LEDs, p. 8). Pressing the key 0, 1 or 2 three times in the graphic mode within 3 seconds will have the following effect:

000 - the · symbol will be displayed at all available items;

111 - the ■ symbol will be displayed at all available items;

222 - reversal of the selection made: the ■ symbol will be displayed at all items where the · symbol was displayed, and the · symbol where the ■ symbol was displayed.

On pressing the ▼ or ▲ key, the keypad will return to the text mode.

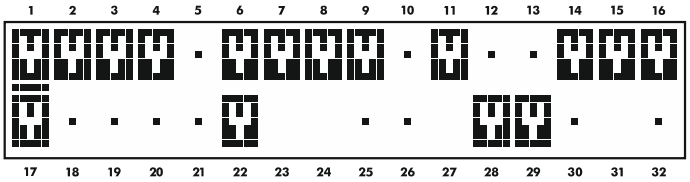


Fig. 3. Example of how information is presented in the graphic programming mode. The blank fields are not available for editing.

Entering decimal and hexadecimal values

Digits are entered by pressing the suitable keys. Characters from A to F are available under the keys with numbers 2 and 3. Keep pressing the keys until the required character appears.

Entering names

Press the particular keys until the required character appears. The characters available in the keypad are shown in Table 3. Hold down the key to display the digit assigned to the key.

Key	Characters available after next keystroke																	
1	!	?	'	`	↵	"	{	}	$	%	&	@	\	^	|	☕	#	1
2	a	b	c	2														
3	d	e	f	3														
4	g	h	i	4														
5	j	k	l	5														
6	m	n	o	6														
7	p	q	r	s	7													
8	t	u	v	·	⏻	■	■	↑	←	→	↓	8						
9	w	x	y	z	9													
0		.	,	:	;	+	-	*	/	=	_	<	>	(	)	[	]	0

Table 3. Characters available when entering names. The lower case letters are available under the same keys (to change the letter case, press ▼ key.

Shown on the left side in the upper line of the display is information about the letter case: [ABC] or [abc] (it will be displayed after pressing any key and will be visible for a few seconds after the last keystroke).

The ▶ key moves the cursor to the right, and the ◀ key – to the left. The ▲ key deletes the character on the left side of the cursor.

5.3.5 Description of user functions

View cleared alarms – available, if the user did not view the violated zones after alarm clearing. It allows to check which zones triggered the alarm. After completion of the viewing, the function is no longer available.

System reset – available to the installer, if the option REQUIRED SYSTEM RESET AFTER VERIFIED ALARM is enabled, and a verified alarm took place. After occurrence of the verified alarm, it is necessary to reset the system by means of this function, in order to make re-arming possible.

Disarm – allows to disarm the partitions accessible to the user from the given keypad.

Clear alarm – allows to silence the alarm.

Clear other alarms – allows to silence the alarms from other objects, to which the user has normally no access.

Abort voice messaging – terminates the telephone messaging.

The messaging can be cancelled automatically together with alarm clearing. The messaging cancellation rules are defined by the installer.

Arm – allows to arm the partitions accessible to the user from the given keypad.

Arm (2 codes) – allows to initiate arming of the partitions which require entering 2 codes.

Disarm (2codes) – allows to initiate disarming of the partitions which require entering 2 codes.

Defer auto-arming – available when auto-arming delay countdown is running. It allows to postpone by a programmed time period the auto-arming of the partition in which the auto-arming delay countdown is running. Entering just zeros will block the auto-arming function (until the next auto-arming time).

Set auto-arming delay – available when the auto-arming delay is programmed for at least one partition and the auto-arming delay countdown is not currently running in that partition. It allows to postpone by a programmed time period the auto-arming of the partition.

Arming mode – allows to select the arming mode which is to be used (the shortcut key is shown in square brackets):

[0] **full arming** (to be used after everybody has left the protected area);

[1] **full arming + bypasses** (allows the users to stay in the protected area) – the zones for which the BYPASSED IF NO EXIT option is enabled by the installer will be bypassed;

[2] **arming without interior** (allows the users to stay in the protected area):

- interior zones (3. INTERIOR DELAYED zone type) will be disarmed;
- violating the exterior zone (8. EXTERIOR zone type) will trigger a silent alarm;
- violating another alarm zone will trigger a loud alarm.

[3] **arming without interior and without entry delay** (allows the users to stay in the protected area – to be used when nobody else is to enter the protected area) – this arming mode is similar to the previous one, but the delayed zones operate as the instant ones (no entry delay).

Cancel 1st code – if the partition is armed/disarmed by means of two codes and the first code has already been entered, the user can still cancel the consent to arming/disarming.

Change own code – allows the user to change his/her own code.

Change telephone code – allows the user to change his/her own telephone code.

Change prefix – available to the administrator, if the use of prefixes in the system has been made available by the installer (the prefix length has been defined). It enables to program the prefixes and the time to remind about the need to change the prefix. Each code will have to be preceded by a prefix:

normal – for everyday use. By default, it consists of a suitable number of digits 0 (e.g. if the determined prefix length is 4, the default prefix is 0000);

DURESS – for use, when the user has been forced to enter the code. Using the code will trigger a silent alarm. By default, it consists of a suitable number of digits 4 (e.g. if the determined prefix length is 3, the default prefix is 444).

Users – the following functions are available in the submenu:

New user – allows to create a new user (see: section ADDING NEW USER p. 28).

Edit user – allows to edit the existing users (see: section EDIT USER p. 28).

Remove user – allows to remove the existing users (see: section REMOVE USER p. 29).

The administrator defines whether the installer is to have access to the USERS submenu (SERV. CAN EDIT option in the CHANGE OPTIONS submenu).

Masters – the submenu provides the following functions available to the installer:

New master – allows to create a new administrator.

Edit master – allows to edit the existing administrators.

Remove master – allows to remove the existing administrators.

Zone bypasses – the following functions are available in the submenu:

Inhibit – allows to temporarily bypass the zones (see: section ZONE BYPASSING (INHIBIT) p. 31).

Isolate – allows to permanently bypass the zones (see: section PERMANENT BYPASSING (ISOLATE) p. 32).

Set time – allows to program the control panel clock. The data are entered in the following format:

time – hour:minute:second,

date – day:month:year.

System state – allows to view the troubles and, if the GRADE 2 global option has been enabled by the installer, also the alarms and bypassed zones, as well as to check the partition status.

Events – the submenu contains functions which allow to view the events saved to the control panel memory (see: section EVENT LOG REVIEWING p. 32).

The content of received SMS messages is also saved to the events log of the INTEGRA 128-WRL control panel.

Reset zones – running the function will result in a temporary deactivation of the 43. RESETABLE POWER SUPPLY type outputs, thus making it possible to reset the alarm memory for detectors supplied from those outputs (e.g. fire detectors).

Clear latched outputs – allows to turn off some of the control panel outputs for which the LATCH option is enabled, as well as the 9. DAY ALARM, 12. SILENT ALARM and 116. INTERNAL SIREN type outputs.

Fin.f.door open – restores the normal operating mode in all modules executing the access control functions (in case of fire, the doors controlled by these modules may be automatically unlocked).

Change options – the following functions are available in the submenu:

Keypad chime – turns on/off the chime signal in the keypad (signaling violations of selected zones).

Outputs chime – allows to block the chime signal from selected partitions on the 11. CHIME type output.

Timers – allows to program parameters of the timers, the editing of which is permitted by the installer.

Partition timers – allows to program the partition timers (see: PROGRAMMING THE PARTITION TIMER p. 34).

No expanders tamper alarms – allows to temporarily disable the expansion module tamper supervision. In case of any problems with the expansion modules, report the fact to the installer.

Permanent service access – the option is available to the master user (administrator). If enabled, the installer has permanent access to the alarm system, which, among other things, enables the control panel to be programmed by using LCD keypad or DLOADX program.

Enabling PERMANENT SERVICE ACCESS option will clear the installer access time programmed with the SERVICE ACCESS function. On the other hand, programming the installer access time will disable the PERMANENT SERVICE ACCESS option.

Service can edit – the option is available to the master user (administrator). If it is enabled, the installer can add, edit and delete users in the administrator's object.

Service arm/disarm/clear/bypass – the option is available to the master user (administrator). If it is enabled, the installer can arm/disarm the system, clear alarms and bypass zones in the administrator object.

Permanent DLOADX access – the option is available to the master user (administrator). If it is enabled, the control panel can be programmed by means of the DLOADX program, irrespective of whether or not the installer has access to the alarm system.

DloadX IP – enables programming the address of the computer, on which the DLOADX program is installed. The address must be set if the control panel is to initiate communication with the DLOADX program through Ethernet, using the TCP/IP protocols (see: description of the ETHM-1 – DLOADX function, available in the DOWNLOADING submenu). It can be entered as a name or IP address.

GuardX IP – enables programming the address of the computer, on which the GUARDX program is installed. The address must be set if the control panel is to initiate communication with the GUARDX program through Ethernet, using the TCP/IP protocols (see: description of the ETHM-1 – GUARDX function, available in the DOWNLOADING submenu). It can be entered as a name or IP address.

Erase service message – allows the user to delete the service message.

Tests – the following functions are available in the submenu:

Partitions – allows to check the status of partitions accessible to the user and operated from the keypad. The partition status is presented by means of a symbol. The numbers placed on the glass allow you to identify the partition numbers. By factory default, the partition status is shown using the following symbols (which can be changed by the installer):

b - temporary blocked,
? - entry delay,
E - exit delay (less than 10 seconds),
e - exit delay (more than 10 seconds),
P - fire alarm,
A - alarm,
p - fire alarm memory,

a - alarm memory,
a - armed,
▪ - disarmed, not ready to be armed (violated zones),
· - disarmed, ready to be armed.

Zones – allows to check the status of zones in the partitions accessible to the user and operated from the keypad. The zone status is presented by means of a symbol. The numbers placed on the glass allow you to identify the zone numbers. On starting the function, the status of zones 1-32 is displayed. Use the ▶ and ◀ keys to display the status of other zones (see also description of the ⊞ LEDs, p. 8). By factory default, the zone status is shown using the following symbols (which can be changed by the installer):

b - zone bypass,
l - trouble "long violation",
f - trouble "no violation",
T - tamper alarm,
A - alarm,
▉ - zone tamper,
▪ - zone violation,
t - tamper alarm memory,
a - alarm memory,
· - zone OK.

Supply voltages – available to the installer. Enables checking of the supply voltage for individual expansion modules.

Temperatures – allows to check the temperatures measured by ATD-100 wireless detectors.

Radio devices – allows to check the radio signal level for ABAX system wireless devices supported by the control panel.

Zone Test – the submenu contains functions which allow to test the detectors connected to the zones (see: section ZONE TESTING p. 34).

Battery test – available to the installer. Upon starting the function, the control panel will generate events to inform about the status of batteries of the control panel and hardwired expansion modules with power supply. Additionally, the status of 60. TECH.-BATTERY LOW type zones will be analyzed.

Manual transmission test – generates an event, which starts the procedure of event transmission to the monitoring station (a code sent with the system identifier).

Monitoring station test (1A, 1B, 2A, 2B) – allows to send a test transmission to the monitoring station (separate functions for each of the telephone numbers). When sending the transmission, messages are displayed to inform about the currently performed operation. The function is useful when starting the reporting or in case of any reporting trouble.

GPRS monit.test – sends a test transmission to the monitoring station via GPRS. When sending the transmission, messages on the display provide information on the currently performed operation. **only INTEGRA 128-WRL**

Messaging test – allows to test the messaging function. Upon starting the function:

1. Enter the number of the telephone (consecutive number on the telephone list).
2. Press the ▼ key.
3. Enter the number of voice message.

4. Press the # key. The control panel will call the indicated number and play back the message.

Answering test – if this function is started, information on the number of rings and going off-hook is displayed when answering the telephone call.

Proximity card test – allows to check the number of proximity card and establish to whom it belongs (if the card belongs to a user of the system).

CA-64 PTSA test – allows to test the mimic board.

View masters – available to the administrator. It makes it possible to check in which objects the master users are created.

Keypad name – allows to check the given keypad name.

File in DLOADX – displays the date and time of writing the data to the control panel by means of the DLOADX program and the name of file with control panel data.

Panel version – displays information on the control panel firmware version.

STM program version – displays information on the program version of the processor used to operate ABAX system and control panel zones. **only INTEGRA 128-WRL**

GSM IMEI/v/sig. – allows to check the level of signal received by the GSM telephone antenna, individual identification number of the telephone, and the telephone version. The ▲ and ▼ keys are to be used for scrolling through the displayed information. **only INTEGRA 128-WRL**

IP/MAC ETHM-1 – displays the local IP address, MAC number and public IP address of the ETHM-1 / ETHM-1 Plus module connected to the control panel (use the ▼ and ▲ keys to scroll the information).

Modules versions – allows to check the firmware versions for devices connected to the control panel communication buses.

Time synchronization – allows to manually start synchronization of the control panel clock and the time server. It applies to the control panel to which the ETHM-1 / ETHM-1 Plus module is connected. The address of time synchronization server must be programmed in the control panel.

i *The function is unavailable, if the time synchronization is running. Automatic time synchronization takes place every day at 05:30.*

Service access – available to the master user (administrator). Allows to program the time period of installer access to the alarm system. The time is programmed in hours. Programming the value 0 means the installer will have no access.

Open door – allows to unlock the door controlled by the alarm system (modules executing the access control functions) or activate the 101. CARD READ – EXPANDER type outputs.

Outputs control – allow to control the devices connected to the MONO SWITCH, BI SWITCH, REMOTE SWITCH, SHUTTER UP and SHUTTER DOWN type outputs (see: section OUTPUTS CONTROL p. 35).

Service mode – available to the installer. Initiates the service mode.

Take SM over – available to the installer. If the service mode has been initiated from another keypad, it can be "taken over", i.e. the service menu can be displayed on the keypad, on which the TAKE SM OVER function has been started.

Downloading – the following functions are available in the submenu:

Start DWNL-RS – available to the installer. Enables the control panel to be programmed locally by means of the DLOADX program.

Finish DWNL-RS – available to the installer. Ends the local programming of control panel.

Start DWNL-MOD. – enables remote programming through an external modem (analog, GSM or ISDN) by means of the DLOADX program.

Start DWNL-TEL – enables remote programming through the built-in 300 bps modem, using the DLOADX program.

Start DWNL-CSD – enables remote programming through the built-in GSM communicator, using CSD technology, by means of the DLOADX program. **only INTEGRA 128-WRL**

Start DWNL-GPRS – enables remote programming through the built-in GSM communicator, using GPRS (General Packet Radio Service), by means of the DLOADX program. **only INTEGRA 128-WRL**

ETHM-1 – DloadX – enables remote programming through the Ethernet (TCP/IP) by means of the DLOADX program. The ETHM-1 (firmware version 1.03 or newer) / ETHM-1 Plus module must be connected to the control panel.

ETHM-1 – GuardX – enables remote operation and administration through the Ethernet (TCP/IP) by means of the GUARDX program. The ETHM-1 (firmware version 1.03 or newer) / ETHM-1 Plus module must be connected to the control panel).

5.4 Arming

This section describes the operations that must be carried out by the user from the keypad in order to initiate the arming procedure. The arming procedure is ended at the running out of the exit delay time (if the procedure is ended successfully, the system becomes armed – see also FAILURE OF ARMING PROCEDURE p. 25). If the exit delay time is 0, the system becomes armed instantly.

The installer can configure the alarm system so that the arming functions will not be available after tamper. A message on the display will indicate that the user must call for service. The arming functions will not be available until the service code is entered and confirmed with the # key.

5.4.1 Full arming without partition selection

The arming without partition selection is possible when none of the partitions to which the user has access is armed and the keypad is not signaling any alarm.

1. Enter the code and confirm with the # key.
2. When the ARM ALL function is displayed, press the # key. The arming procedure will be initiated in all partitions which are accessible to the user and are operated by the keypad.

If the user can only arm one partition, the arming procedure will be initiated as soon as the code is entered and confirmed with the # key.

5.4.2 Full arming the selected partitions

1. Enter the code and confirm with the * key.
2. Using the ▼ key, scroll through the menu until you find the ARM function.
3. Press the # key. A list of partitions which can be armed will be displayed.
4. Using the ▼ and ▲ keys, find in the list the partition which is to be armed (or press 0 key and enter the partition number).
5. Press one of the digit keys 1 to 9. The · symbol in the upper right-hand corner will be replaced by the ■ symbol (see also section SELECTION FROM THE MULTIPLE-CHOICE LIST p. 16).
6. Repeat the steps 4 and 5 for the next partitions which are to be armed.
7. Having selected the partitions which are to be armed, press the # key.

You can also arm the selected partitions using of the ARM SELECTED function, available upon entering the code and confirming with the # key, but only when none of the partitions accessible to you is armed and the keypad is signaling no alarm.

5.4.3 Arming in the selected mode

1. Enter the code and confirm with the * key.
2. Using the ▼ key, scroll through the menu until the ARMING MODE function is found.
3. Press the # key. A list of arming modes will be displayed (see: description of the ARMING MODE function, p. 18).
4. Using the ▲ and ▼ keys, find the arming mode which is to be activated, and then press the # key.
5. When the ARM function is displayed, press the # key. Proceed in the same way, as for the full arming of selected partitions (steps 4-7).

5.4.4 Quick arming

The installer can permit the arming without user authorization. The partitions indicated by the installer will be armed.

1. Select the arming mode (press one of the keys: 0 – full arming; 1 – full arming + bypasses; 2 – arming without interior; 3 – arming without interior and without entry delay).
2. Press the # key. The arming procedure will begin.

5.4.5 Denial of arming

The installer can program the control panel so that the arming procedure could not be started, if:

– a zone is violated in the partition;
– there is a trouble in the system (including tamper);
– there was a verified alarm.

The keypad will inform you about the refusal to arm by means of a message specifying the cause for refusal.

If after a verified alarm the arming is impossible, the installer must be called. The arming will only be possible after the installer intervention (see: description of the SYSTEM RESET function, p. 18).

Bypassing violated zones when arming

If the arming procedure could not be started, and a message on the display informs you that there are violated zones, you can review the list of such zones upon pressing the 2 key. To scroll through the list, use the ▼ and ▲ keys. Pressing the 4 key will allow you to bypass the given zone. A message on the display will prompt you to press the 1 key to confirm that the zone is to be bypassed.

Forced arming

If the arming procedure could not be started, the displayed message can allow of the forced arming (1=Arm). On pressing the 1 key, the system will be armed despite a violated zone or a trouble.

5.4.6 Failure of arming procedure

If the installer has enabled the GRADE 2 option, the arming procedure may end in failure. The system will not be armed, if at the end of the exit delay countdown:

– there is a violated zone in partition which was not violated when the arming procedure was started;
– there is a trouble which did not exist when the arming procedure was started.

5.4.7 Shortening the exit delay time

If such an option is permitted by the installer, the partition exit delay time may be shortened upon pressing in turn the 9 and # keys.

5.5 Disarming and alarm clearing

Enter the code and confirm with the # key (see: section [CODE]# – ARMING / DISARMING MENU p. 10). If only selected partitions are to be disarmed (DISARM SELECTED function), the partitions should be selected in the same way as when arming the selected partitions.

5.5.1 Alarm clearing without disarming

1. Enter the code and confirm with the ✻ key.
2. Using the ▼ key, scroll through the menu until the CLEAR ALARM function is found.
3. Press the # key.

5.6 Two-code arming / disarming

If the partition is to be armed / disarmed with 2 codes, the user entering the first code must:

1. Enter the code and confirm with the ✻ key.
2. Scroll through the menu using the ▼ key until the ARM (2 CODES) / DISARM (2CODES) function is found.
3. Press the # key. Proceed in the same way as for the full arming of selected partitions (steps 3-7).
4. If the installer has not set the code validity at 60 seconds, specify the code validity and confirm with the # key.

Prior to expiration of the code validity, the user entering the second code must arm / disarm the partition using the:

- LCD keypad (see: section ARMING or DISARMING AND ALARM CLEARING);
- partition keypad ([*code*]#);
- reader (read-in of proximity card or DALLAS iButton).

The installer can configure the alarm system so that the second code will have to be entered on another LCD keypad, partition keypad, etc.

5.7 Triggering the alarm from keypad

The installer can permit triggering alarms from the keypad. To trigger an alarm, do the following:

fire alarm – press the 🔥 key for approx. 3 seconds;

medical (auxiliary) alarm – press the ⓘ key for approx. 3 seconds;

panic alarm – press the key for approx. 3 seconds. The installer defines whether the loud panic alarm (setting off the loud alarm signal) or the silent panic alarm (without the loud signal) will be triggered.

5.8 Users

The users can be added, edited and removed by:

- master user (administrator);
- installer (if the SERV. CAN EDIT option is enabled by the administrator);
- user (if granted the USERS EDITING right).

The following data can be defined for the user:

Code – a sequence of digits for authorization of the user when using keypads and code locks. The control panel supports codes consisting of 4 to 8 characters, however the installer can define the minimum length of the code.

Telephone code – a sequence of digits for authorization of the user when using the functions of telephone call answering and telephone control (see: section CALL ANSWERING AND TELEPHONE CONTROL p. 43).

Partitions – partitions to which the user has access (i.e. he is authorized to arm or disarm them, clear alarms etc.).

Type – see: section USER TYPES p. 27.

User schedule – parameter for the SCHEDULED type code (see: section USER TYPES p. 27).

Validity time – parameter for the RENEWABLE, TEMPORARY or SCHEMATIC type codes (see: section USER TYPES p. 27).

Blocking time – parameter for the BLOCKING PARTITION type code (see: section USER TYPES p. 27).

Rights – define which functions can be used by the user. The following rights (permissions) are available:

- Arming
- Disarming
- Disarm, when other user arm [Can alw.disarm] – if the user does not have this right, he/she can only disarm the system if it was armed by him/her
- Partition alarm clearing [Alarm clearing]
- Object alarm clearing [Object al.clr.]
- Other objects alarm clearing [Other al.clr.]
- Telephone messaging canceling [V.msg.clearing]
- Auto-arming defer [Arm deferring]
- First code for two codes partition [Enter.1st code]
- Second code for two codes partition [Enter.2nd code]
- Access temporary blocked partitions [Block p.access]
- Change access code [Code changing]
- Users editing
- Zones bypassing [Zones inhibit]
- Zone isolation [Zones isolate]
- Clock setting
- Trouble state checking [Troubles view.]
- Event log reviewing [Events viewing]

- Detectors resetting [Zones resett.]
- Options programming [Options chang.]
- Access to menu TEST [Tests]
- Downloading starting [Downloading]
- Access to BI & MONO outputs [Outs control]
- System state review in GUARDX [GuardX using]
- Resetting outputs [Clr.latch.outs]
- Simple user – having entered the code, confirmed with the # key, the user never selects the partitions which are to be armed / disarmed. All partitions the user has access will be armed / disarmed.
- Administrator – the user has access to the menu functions which are reserved for the administrator

Keypads etc. – additional modules from which the user will be able to operate the system (proximity card arm/disarm devices, partition keypads, code locks, reader expanders).

Proximity cards / DALLAS chips – if the proximity card / DALLAS iButton reader is used in the system, a proximity card / DALLAS iButton can be assigned to the user, which will allow the user to operate the system by means of readers.

Keyfobs – in case of the INTEGRA 128-WRL control panel or any other control panel to which a module with keyfob support is connected (ACU-120, ACU-270, ACU-100, ACU-250, INT-RX or INT-RX-S), a keyfob can be assigned to the user, which will allow to operate the system remotely. The user may have up to 2 keyfobs: the APT-100 (supported by the ABAX system) and the 433 MHz (supported by the INT-RX or INT-RX-S modules).

Buttons – the button functions are available, if a keyfob has been assigned to the user. It is possible to assign a zone to a keyfob button or combination of buttons. The zone will be violated upon pressing the button / combination of buttons. The assigned zone should not exist physically.

Events (RX) / **Events (ABAX)** – if a keyfob has been assigned to the user, it is possible to define whether pressing the appropriate keyfob button will result in logging an event which informs that the keyfob has been used.

ABAX confirmation – if an ABAX system keyfob has been assigned to the user, it is possible to determine the status of which outputs will be presented on the keyfob LEDs on pressing any button.

Name – individual user name.

5.8.1 User types

The name as used in the keypad is shown in the square brackets. The description includes only the codes, but the information provided below applies to all identifiers assigned to the user.

Normal – basic type of user.

One-time [Single] – the user will get one-time access.

Renewable [Time renewable] – the user has access to the system for a defined period of time. The user validity time should be defined. Before the validity time expires, the control panel will prompt the user to change the code. After the code has been changed, the validity time will run from the beginning.

Temporary [Time not renew.] – the user has access to the system for a defined period of time. The user validity time should be defined. After the validity time expires, the user will have no access to the system.

Duress – code to be used in hold-up and duress situations. Use it to trigger a silent alarm and send the event code to the monitoring station.

"Mono" output operating [Mono outputs] – code for control of the MONO SWITCH type outputs.

"Bi" output operating [Bi outputs] – code for control of the BI SWITCH type outputs.

Blocking partition [Part.temp.block.] – the code enables access to the armed partitions. Using the code will block the armed partition(s) (the partition zones will not trigger the burglary alarm). The blocking time is defined individually for each user within the range from 1 to 109 minutes. If, however, the time of bypassing for guard round is defined for the partition and its duration is longer, the blocking will last longer.

Cash machine zones bypassing [Acces.to cash m.] – the code to be used to unblock access to the cash dispenser (the 24H CASH MACHINE type zones will be temporarily bypassed in the partition).

Guard – using this code means having made the round (additionally, it can result in the partition being temporarily bypassed for the duration of guard round). The installer defines the modules which are used to confirm making the round and determines the time interval between successive rounds. If such a user is granted access to the partition, he/she will have the same possibilities as the NORMAL type user.

Scheduled – the user has access to the system as per the time schedule for a specified period of time. It is necessary to select the schedule (the schedule is programmed by the installer) and define the user validity period.

5.8.2 Adding new user

1. Enter the code and confirm with the ✱ key.
2. Press in turn the 2 and 1 keys. The list of functions to define the user parameters will be displayed.

If the service code has been entered, before the list of functions is displayed, it is necessary to specify the object in which the new user is to be created (the service code enables access to all objects).

3. Using the appropriate functions, define the user's parameters.

At least one identifier, i.e. code, proximity card, DALLAS iButton or keyfob, must be assigned to the user.

The new user may not be granted a higher authority level than the person who is adding that user to the system.

4. Press the ✱ key.
5. When a prompt appears, asking you if the changes are to be saved, press the 1 key.
6. A message will inform you that a new user has been created. Press the ✱ key to return to the USER submenu.

5.8.3 Edit user

The user can edit the users in relation to which he/she is the superior. For example, if the user A has created the user B, and the user B has created the user C, then the user A can edit the users B and C.

The user being edited may not be granted a higher authority level than the person who is editing such a user.

1. Enter the code and confirm with the ✱ key.
2. Press the 2 key twice. The list of users will be displayed.

3. Using the ▼ and ▲ keys, find in the list the user who is to be edited.
4. Press the # key. The list of functions for defining the user's parameters will be displayed.
5. Using appropriate functions, modify the user's parameters.
6. Press the ✻ key.
7. When a prompt appears, asking you if the changes are to be saved, press the 1 key.
8. A message will inform you that the user has been modified. Press the ✻ key to return to the list of users.

5.8.4 Removing a user

The user can remove the users in relation to which he/she is the superior. For example, if the user A has created the user B, and the user B has created the user C, then the user A can remove the users B and C.

1. Enter the code and confirm with the ✻ key.
2. Press in turn the 2 and 3 keys. The list of users will be displayed.
3. Using the ▼ and ▲ keys, find in the list the user who is to be removed.
4. Press the # key. A message will inform you that the user has been removed.
5. Press the ✻ key to return to the list of users.

5.8.5 Adding proximity card / DALLAS iButton

1. When adding or editing a user, run the NEW PROX. CARD / NEW DALLAS function.
2. Using the ▼ and ▲ keys, select how the card / iButton is to be added. The number of card / iButton can be read by a selected reader (device equipped with a reader) or entered manually.
3. Press the # key.
4. If the number of card / iButton is to be read, read in the card / iButton twice, following the instructions appearing on the keypad display. When the read number of card / iButton is displayed, press the # key.
5. If the number of card / iButton is to be entered, enter it from the keypad, and then press the # key.
7. You will be brought back to the list of functions for defining the user parameters. Instead of the NEW PROX. CARD / NEW DALLAS function, the REMOVE PROX. CARD / REMOVE DALLAS function will be available. Press the ✻ key.
6. When a prompt appears, asking you if the changes are to be saved, press the 1 key.

Proximity cards / DALLAS iButtons are added to the master users (administrators) in the same way.

5.8.6 Adding keyfob

1. When adding or editing a user, run the NEW RX KEYFOB / NEW ABAX KEYFOB function (depending on which keyfob is to be added).
2. Using the ▼ and ▲ keys, select how the keyfob is to be added. The number of keyfob can be read during transmission by a device supporting keyfobs or entered manually.
3. Press the # key.
4. If the keyfob number is to be read, press twice the keyfob button according to the instructions displayed on the keypad. When the keyfob number is displayed, press the # key.
5. If the keyfob number is to be entered, enter it from the keypad, and then press the # key.

6. You will be brought back to the list of functions for defining the user parameters. Instead of the NEW RX KEY FOB / NEW ABAX KEYFOB function, the REM. RX KEY FOB / REM.ABAX KEYFOB function will be available. Additionally, some functions appear to allow you to configure the keyfob.

Prior to assigning the zones to buttons / combinations of buttons, consult the installer.

Numeration of the keyfob buttons and LEDs is described in section OPERATING THE ALARM SYSTEM BY MEANS OF KEYFOB (p. 45).

7. Using the ▼ key, find the BUTTON 1 function in the list, and then press the # key.
8. Using the ▼ and ▲ keys, select which zone is to be violated on pressing the 1 button in the keyfob (you can also enter the zone number from the keypad), and then press the # key.
9. Repeat the steps 7 and 8 for other buttons / combinations of buttons which are to be used.
10. Using the ▼ key, find the EVENTS (RX) / EVENTS (ABAX) function in the list.
11. Press the # key. The list of buttons / combinations of buttons will be displayed. In the upper right-hand corner of the display, an additional symbol is located:
    - ▣ – pressing the button / combination of buttons is written to the event log (default setting);
    - ▪ – pressing the button / combination of buttons is not written to the event log.
12. Define whether pressing the button / combination of buttons will be written to the event log (see: section SELECTION FROM THE MULTIPLE-CHOICE LIST p. 16), and then press the # key.
13. For the APT-100 (ABAX) keyfobs, use the ▼ key to find the ABAX CONFIRMAT. function in the list, and then press the # key.
14. A list will be displayed showing the outputs which have been assigned by the installer for confirmation (maximum 8). Select up to 3 of them (see: section SELECTION FROM THE MULTIPLE-CHOICE LIST p. 16). Upon pressing any keyfob button, information on the status of selected outputs will be presented on the keyfob LEDs for a few seconds. Thus you can get confirmation that the function has been executed or information on the current status of the system.

The installer can define the list of outputs by means of the keypad (ABAX CONFIRMAT. function [SERVICE MODE ▶STRUCTURE ▶HARDWARE ▶EXPANDERS ▶ABAX CONFIRMAT.] or a computer with the DLOADX program ("Keyfobs ABAX" window).

15. Press the # key.
16. Press the * key.
17. When a prompt appears, asking you if the changes are to be saved, press the 1 key.

Keyfobs are added to the master users (administrators) in the same way.

5.8.7 Removing keyfob

1. When adding or editing a user, run the REM. RX KEY FOB / REM.ABAX KEYFOB function (depending on which keyfob is to be removed). The appropriate function is only displayed when a keyfob has already been assigned to the user.
2. When the keyfob number and a prompt whether the keyfob is to be removed are displayed, press the 1 key. You will be brought back to the list of functions for defining the user parameters.
3. Press the * key.
4. When a prompt appears, asking you if the changes are to be saved, press the 1 key.

Removal of a keyfob will not erase its settings (dependences between the buttons and zones, confirmation rules, etc.). When added to the user, the new keyfob will have the same settings as the deleted one.

The installer can remove all keyfobs, including their settings, by means of the functions available in the service mode (▶STRUCTURE ▶HARDWARE ▶EXPANDERS ▶REM.RX KEY FOBS / REM.ABAX KEYFOB).

The administrators' keyfobs are removed in the same way.

5.9 Master users (administrators)

The master users (administrators) can be added, edited and removed by the installer. There can be 1 administrator in each object. The administrator has access to all partitions in the object and also specifies how the system can be accessed by using the service code. Most of the parameters which are defined for the ordinary user can be defined for the administrator (see: section USERS p. 26).

5.10 Zone bypassing

You can bypass / unbypass zones in the disarmed partitions. Violating a bypassed zone will not trigger any alarm. Bypassing the zones is useful in case of damage or failure of the detector connected to the zone, which results in malfunctioning of the alarm system (e.g. triggering false alarms).

Zone bypassing reduces the level of protection. Prior to arming, make sure that there are no accidentally bypassed zones in the partition, which might allow an intruder to get access to the protected area despite arming.

If a zone is bypassed, call in the installer (service technician) immediately to repair the defect.

For security considerations, the installer may reduce the number of zones that the user will be allowed to bypass.

5.10.1 Zone inhibiting

The zones can be inhibited by the users having the ZONES BYPASSING right. The inhibited zone will be bypassed until the partition to which the zone belongs is disarmed, or until the zone is unbypassed by the user.

1. Enter the code and confirm with the ✱ key.
2. Press in turn the 4 and 1 keys. The list of zones will be displayed. There is an additional symbol in the upper right-hand corner of the display to inform you about the given zone status:
   - ▪ – the zone is not bypassed;
   - ⊡ – the zone is inhibited;
   - ▦ – the zone is isolated.
3. Using the ▼ and ▲ keys, find in the list the zone which is to be inhibited (or press 0 key and enter the zone number).
4. Press one of the digit keys 1 to 9 until the ⊡ symbol appears in the upper right-hand corner of the display.
5. Repeat the steps 3 and 4 for the next zones which are to be inhibited.

6. Press the # key. A message will inform you that the zones are inhibited.

Having started the INHIBIT function (step 2), you can press the ▶ or ◀ key to switch over the keypad to the graphic programming mode (see: section SELECTION FROM THE MULTIPLE-CHOICE LIST p. 16).

5.10.2 Zone isolating

The zones can be isolated by the users having the ZONES BYPASSING and ZONE ISOLATION rights. The isolated zone will remain bypassed until unbypassed by the user.

1. Enter the code and confirm with the ✱ key.
2. Press in turn the 4 and 2 keys. The list of zones will be displayed. There is an additional symbol in the upper right-hand corner of the display to inform you about the given zone status:
   - ▪ – the zone is not bypassed;
   - ▪ – the zone is inhibited;
   - ▪ – the zone is isolated.
3. Using the ▼ and ▲ keys, find in the list the zone which is to be isolated (or press 0 key and enter the zone number).
4. Press one of the digit keys 1 to 9 until the ▪ symbol appears in the upper right-hand corner of the display.
5. Repeat the steps 3 and 4 for the next zones which are to be isolated.
6. Press the # key. A message will inform you that the zones are isolated.

Having started the ISOLATE function (step 2), you can press the ▶ or ◀ key to switch over the keypad to the graphic programming mode (see: section SELECTION FROM THE MULTIPLE-CHOICE LIST p. 16).

5.10.3 Unbypassing

The zones can be unbypassed by the users having the ZONES BYPASSING right. Proceed in the same way as when inhibiting or isolating the zones (steps 1-3), but the ▪ symbol must be shown in the upper right-hand corner of the display, if the zone is to be unbypassed upon pressing the # key.

5.11 Viewing the event log

The events viewing function, when started by the administrator or the ordinary user, provides no information about:

- *panic alarms;*
- *alarms triggered using the DURESS type code.*

5.11.1 Viewing all events

1. Enter the code and confirm with the ✱ key.
2. Press in turn the 5 and 2 keys. The last event which occurred in the system will be displayed.
3. Using the ▲ key, scroll through the list of previous events.

5.11.2 Viewing the events required for Grade 2

If the GRADE 2 option is enabled in the system, the function allowing the installer and administrators to view events required by EN 50131 for Grade 2 is available.

1. Enter the code and confirm with the ✻ key.
2. Press the 5 key. Functions available in the EVENTS submenu will be displayed.
3. Using the ▼ key, scroll the menu until the GRADE2 function is found.
4. Press the # key. The last Grade 2 required event which occurred in the system will be displayed.
5. Using the ▲ key, scroll through the list of previous events.

5.11.3 Viewing the selected events

1. Enter the code and confirm with the ✻ key.
2. Press in turn the 5 and 1 keys.
3. When the SELECT EVENTS function is displayed, press the # key. The list of event types will be displayed.
4. Select which event types are to be displayed (see: section SELECTION FROM THE MULTIPLE-CHOICE LIST p. 16).
5. Press the # key. This will bring you back to the SELECTED submenu.
6. Using the ▼ key, scroll down the menu until you find the VIEW function.
7. Press the # key. The last one of the selected events which occurred in the system will be displayed.
8. Using the ▲ key, scroll through the list of previous events.

In addition to defining the event types to be displayed, the SELECT PART. function can also be used to indicate the partitions to which the events are to refer.

If the GRADE 2 option is enabled in the system, the installer or administrator can use the VIEW GRADE2 function instead of the VIEW function. In such a case, the events selected among those required by the EN 50131 standard for Grade 2 will be displayed.

5.11.4 Way of presenting events

The following information is shown in the display upper line:

- date and time of event occurrence;
- additional information on the events in shortened form, e.g. number of partition, zone, user, timer, expander, keypad, etc.

Event description is displayed in the lower line.

If no key is pressed for a few seconds, additional information on the event will be displayed, e.g. name of partition, zone, user, timer, expander, keypad, etc. After a few seconds, the event description will be displayed again, and so on.

Pressing the ▶ key enables the manual toggling between description of the event and additional information on the event.

Pressing the ◀ key when the event description is displayed will allow you to see further additional information on the event, shown in a shortened form.

Using the ◀ or ▶ key will block the automatic toggling between description of the event and additional information on the event.

After the list of events has been scrolled through with the use of the ▲ or ▼ key, the automatic toggling between description of the event and additional information on the event will be restored.

5.12 Programming the partition timer

The partition timer automatically arms / disarms the partition.

1. Enter the code and confirm with the ✻ key.
2. Using the ▼ key, scroll through the menu until you find the CHANGE OPTIONS submenu.
3. Press the # key.
4. Using the ▼ key, scroll through the menu until you find the PART. TIMERS function.
5. Press the # key. The list of partitions will be displayed.
6. Using the ▼ and ▲ keys, find in the list the partition for which the timer is to be programmed.
7. Press the # key.
8. When the ACTIVE option is displayed, make sure it is enabled (the ☑ symbol is displayed next to the option). If it is not enabled (the ☐ symbol is displayed next to the option), press any digit key.
9. Using the ▼ key, scroll through the menu until you find the TYPE function.
10. Press the # key.
11. Using the ▼ and ▲ keys, select the timer type:
    everyday – if the partition is to be armed / disarmed at the same time every day;
    weekly – if the partition is to be armed / disarmed at different times on different days of the week.
12. Press the # key.
13. If you have selected the daily variant, the function will allow you at once to program the arming time, and upon pressing the ▲ or ▼ key – the disarming time. Upon confirmation with the # key, you will be brought back to the list of options and functions.
14. If you have selected the weekly variant, you will be brought back to the list of options and functions, where functions will appear to enable programming of the arming / disarming time for each day of the week (in the same way as for daily timer).

i *Programming the value 99:99 means that the partition will not be armed / disarmed.*

15. After the arming time has been programmed, an additional function will be displayed, which allows you to define which arming mode will be activated by the given timer. By default, the timer activates the full arming mode. If another arming mode is to be activated, run this function (for the daily timer or individually for each day of the week) and, using the ▲ and ▼ keys, select another arming mode. Confirm, using the # key.
16. Having programmed all parameters, press the ✻ key.
17. When a prompt appears, asking you if the changes are to be saved, press the 1 key.

5.13 Zone testing

Within periodic inspections of the security alarm system, the detectors must be checked for proper functioning. The zone testing function will allow you to do it without triggering the reaction normally expected on violation, which is of particular importance in case of permanently armed zones.

1. Enter the code and confirm with the ✻ key.
2. Using the ▼ key, scroll through the menu until you find the TESTS submenu.

3. Press the # key.
4. Using the ▼ key, scroll through the menu until you find the ZONES TEST submenu.
5. Press the # key.
6. When the NEW function is displayed, press the # key.
7. Select whether burglary zones or fire and technical zones will be tested, and then press the # key.
8. Select the partitions in which zones will be tested (see: section SELECTION FROM THE MULTIPLE-CHOICE LIST p. 16).
9. Specify the test duration (maximum 50 minutes) and press the # key.
10. Define, whether violation of a zone is to be signaled by chime in the keypad (the signaling will be enabled upon pressing any digit key – the symbol will be displayed).
11. Press the # key. The zone test will start.

Beginning of the zone test in any partition will start the test mode in all ABAX system wireless devices which are used together with the control panel (the wireless detectors will signal violations by means of LEDs).

If any detectors with remote LED ON/OFF function are connected to the control panel, you can switch on the LEDs in them for the test duration (the installer can configure the control panel so that this will take place automatically at the beginning of the test).

You can terminate the zone test before expiration of the programmed time, using the FINISH TEST function (▶TESTS ▶ZONE TEST ▶FINISH TEST). Up to 6 seconds can elapse between starting the function to the actual end of the test (during this the FINISH TEST function will be still available).

12. Depending on the type of tested detector:
    - magnetic contact – open and close the door or window protected by means of the magnetic contact;
    - motion detectors – pass in front of the detector;
    - other detectors – follow the manufacturer's directions for the detector testing.
13. Look through the test results. To do so, enter again the ZONES TEST submenu (see: steps 1-5) and start the VIEW RESULTS function. You can scroll through the list of results, using the ▲ and ▼ keys. Press the ▶ or ◀ key to switch over the display to the graphic mode, in which information is provided by means of symbols:
    - · - zone was not violated,
    - - zone was violated.

    Pressing the ▶ or ◀ key in the graphic mode will display information on another set of zones (see also description of the LEDs, p. 8).

The test results can be deleted by means of the CLEAR RESULTS function (▶TESTS ▶ZONES TEST ▶CLEAR RESULTS).

5.14 Outputs control

If permitted by the installer, the control function can be started without user authorization, upon pressing in turn the 8 and # keys.

1. Enter the code and confirm with the * key.

2. Press the 8 key. Depending on how the control panel has been configured by the installer:
   - a group of outputs will be displayed – using the ▼ and ▲ keys, find the group which includes an output, and then press the # key to display the list of outputs;
   - the list of controllable outputs will be displayed at once.
3. Using the ▼ and ▲ keys, find in the list the output whose status you want to change to control the device connected to the output. The output status is presented by means of symbols:
   - ▪ - output inactive (disabled),
   - ▪ - output active (enabled).

The output status can be presented according to the zone status. The displayed symbols should then be interpreted as follows:

- ▪ - *zone not violated (the device controlled by output is inactive);*
- ▪ - *zone violated (the device controlled by output is active).*

The way of presenting the status of roller shutter outputs differs from how the status of other outputs is presented (see: section CONTROLLING THE ROLLER SHUTTER OUTPUTS).

5.14.1 Controlling the MONO SWITCH type of output

When the output is inactive:
- pressing the ▶ key will activate the output for the time programmed by the installer;
- pressing the # key will allow you to program the time for which the output will be activated upon the next pressing of the # key.

When the output is active, pressing any digit key will turn the output off.

5.14.2 Controlling the BI SWITCH type of output

Pressing the # or ▶ key will change over the output status. Additionally, when the output is active, pressing any digit key will turn the output off.

5.14.3 Controlling the REMOTE SWITCH type of outputs

Depending on how the output has been programmed, pressing the # or ▶ key will activate the output for the time programmed by the installer or change over the output status. Additionally, when the output is active, pressing any digit key will turn the output off.

5.14.4 Controlling the roller shutter outputs

The SHUTTER UP and SHUTTER DOWN type of outputs are always programmed as consecutive and in pairs. Displayed on the list of outputs is only the name of output programmed as SHUTTER UP. The status of outputs is presented by means of symbols:

- ▪ - outputs inactive (off),
- ↑ - SHUTTER UP output active (on),
- ↓ - SHUTTER DOWN output active (on).

Pressing the # or ▶ key will display the cursor in the form of a horizontal line under the output status symbol. Pressing the ▲ key will turn on the SHUTTER UP type output (if both outputs are inactive) or turn off the SHUTTER DOWN type output (if it is active). Pressing the ▼ key will turn on the SHUTTER DOWN type output (if both outputs are inactive) or turn off the SHUTTER UP type output (if it is active). Irrespective of which output is currently active, pressing any digit key will turn the output off. When the control is finished, press the # or ◀ key to return to the list of outputs which can be controlled (the cursor under the symbol will disappear).

6. Using the partition keypad

The main task of the partition keypad is to arm/disarm one partition. Additionally, it offers a number of other functions, including e.g. the access control (supervision of a single door).

SATEL offers the following partition keypads:

INT-S;

INT-SK;

INT-SCR (multifunction keypad, offering the partition keypad functionality).

The keypads are available with keys backlight in various color versions. The color version is indicated by an additional letter symbol included in the keypad designation (e.g. INT-S-GR – green backlight; INT-S-BL – blue backlight).

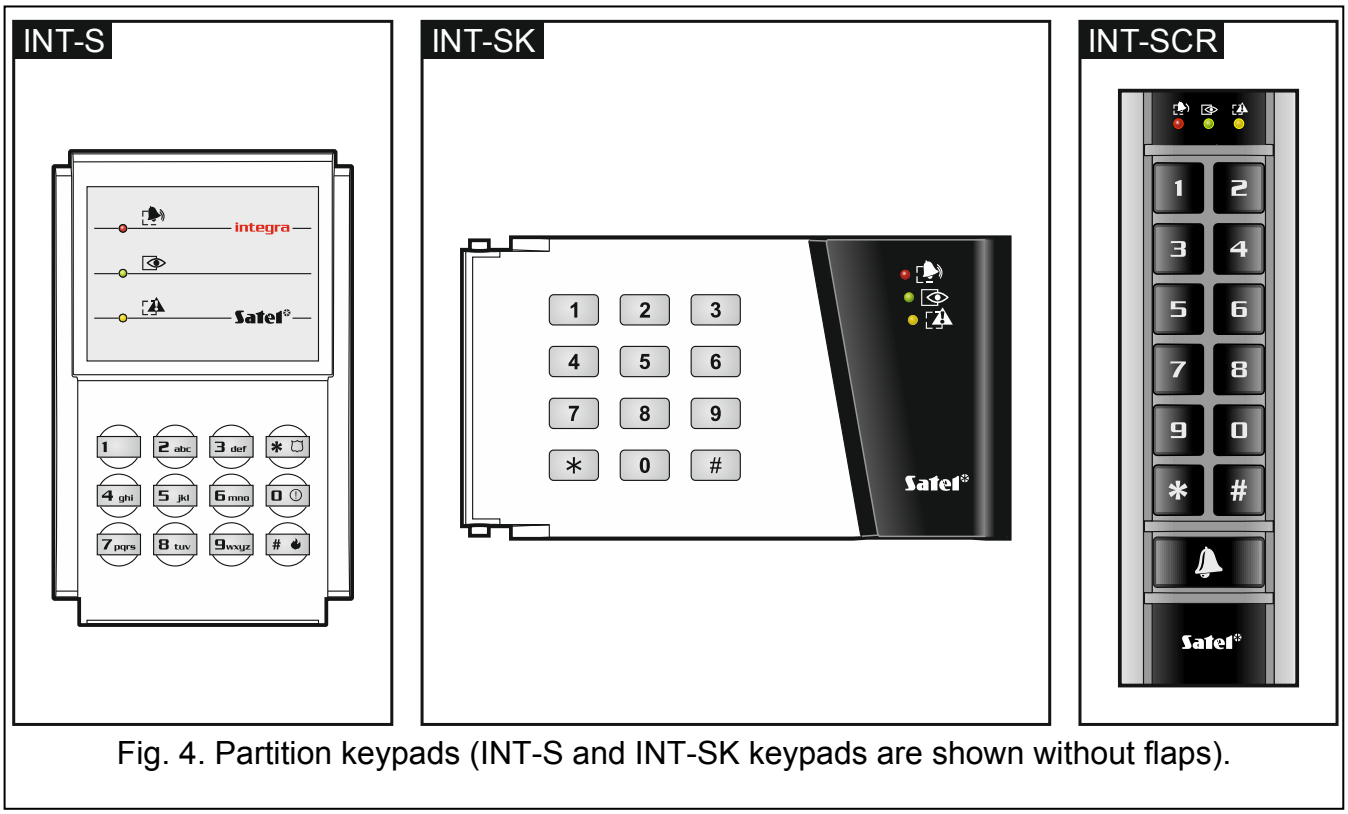


Fig. 4. Partition keypads (INT-S and INT-SK keypads are shown without flaps).

6.1 Description of partition keypads

6.1.1 LED indicators

LED	Color	Function description
	green	**ON** – partition armed
	red	**ON** or **blinking** – alarm or alarm memory
	yellow	**blinking** – trouble or trouble memory

Table 4. Description of LEDs in partition keypads.

Information on the armed status can be extinguished after the time period defined by the installer.

If the installer has enabled the GRADE 2 option:

– *the LED will not inform about the alarms;*

– *blinking of the ⚠ LED means that there is a trouble in the system, some zones are bypassed, or that there was an alarm.*

The 👁 and ⚠ LEDs blinking alternately indicate that the system is waiting for the second code during the two code arming / disarming.

All LEDs blinking in turn indicate that there is no communication with the control panel.

6.1.2 Keys

The keys enable authorization of the user by means of code and running of the functions available from the partition keypad.

In the INT-SCR keypad, the 🔔 button is additionally available. It controls the keypad OC type output (the output is active, when the button is pressed).

6.1.3 Built-in proximity card reader

The INT-SCR keypad has a built-in reader which enables operation by means of proximity cards (proximity tags or other 125 kHz passive transponders). The installer determines, if the reader will be operated.

Presenting the card is interpreted in the same way as entering the code and confirming with the * key. Holding the card (for approx. 3 seconds) is interpreted in the same way as entering the code and confirming with the # key.

6.1.4 Sound signaling

Beeps generated when operating

The installer can disable the sound signaling or replace it with blinking of the keys backlight.

1 short beep – pressing any digit key, confirmation that code has been entered or card has been read.

2 short beeps – acceptance of the first code during two code arming / disarming.

3 short beeps – signaling of:

– starting the procedure of arming (there is exit delay in the partition) or arming (there is no exit delay in the partition),
– disarming and/or alarm clearing.

4 short and 1 long beeps – confirmation that the function has been executed.

3 pairs of short beeps – the user should change his/her code.

1 long beep – refusal to arm (there are violated zones in the partition or there is a trouble).

2 long beeps – unknown code/card.

3 long beeps – unavailable function.

Events signaled by sounds

Only installer selected events are signaled.

Alarms are signaled for the time programmed by the installer.

5 short beeps – zone violation (CHIME).

Long beep every 3 seconds, followed by a series of short beeps for 10 seconds and 1 long beep – countdown of exit delay (if the time is shorter than 10 seconds, only the final sequence of short beeps will be generated).

A sequence of 7 beeps of diminishing duration, repeated every few seconds – countdown of auto-arming delay.

2 short beeps every second – countdown of entry delay.

Continuous beep – alarm.

Long beeps every 2 seconds – alarm memory.

Long beep every second – fire alarm.

Short beeps every 2 seconds – fire alarm memory.

Very short beeps – door open too long.

6.2 Functions available from the partition keypad

6.2.1 [Code]*

Depending on the user type and authority level, keypad settings and the alarm system status, entering the code and confirming with the * key will execute one or a few of the following functions:

- unlocking the door (activating the relay);
- disarming the partition;
- clearing alarm;
- changing over the status of 25. BI SWITCH type outputs;
- turning on the 24. MONO SWITCH type outputs;
- guard round confirmation;
- enabling temporary partition blocking.

Most of the abovementioned functions are available after enabling the LOCK [LOCK FEATURE] option for the partition keypad. Whether the functions are available may also depend on the other keypad options (e.g. if the lock operates in the ON IF PARTITION ARMED [ON IF PART.ARMED] mode, most of the functions will be unavailable).

6.2.2 [Code]#

Depending on the user type and authority level, keypad settings and the alarm system status, entering the code and confirming with the # key will execute one or a few of the following functions:

- starting the partition arming procedure / arming;
- disarming the partition;
- clearing alarm;
- changing over the status of 25. BI SWITCH type outputs;
- turning on the 24. MONO SWITCH type outputs;
- guard round confirmation;
- enabling temporary partition blocking;
- unblocking cash machine access.

6.2.3 Quick arming

The installer can permit arming without the user authorization.

1. Select the arming mode (press one of the keys: 0 – full arming; 1 – full arming + bypasses; 2 – arming without interior; 3 – arming without interior and without entry delay).
2. Press the # key. The arming procedure will begin.

6.2.4 Triggering the alarm from keypad

The installer can permit triggering alarms from the keypad. To trigger an alarm, do the following:

fire alarm – press the [# 🔥] (INT-S) / [*] (INT-SK) / [#] (INT-SCR) key for approx. 3 seconds;

medical (auxiliary) alarm – press the 0 key for approx. 3 seconds;

panic alarm – press the [* 🔔] (INT-S) / [#] (INT-SK) / [*] (INT-SCR) key for approx. 3 seconds. The installer defines whether the triggered alarm will be loud (setting off the loud alarm signaling) or silent (without loud signaling).

6.2.5 Silencing the alarm sound at the keypad

If the keypad is signaling alarm, pressing any digit key will silence the signaling for approx. 40 seconds.

6.2.6 Code changing

The installer can permit the change of own code by means of the partition keypad.

1. Press the 1 key for 3 seconds.
2. When the 🔔 and 👁 LEDs start blinking alternately, enter the old code and confirm it with the # key.
3. When the 🔔 and ⚠ LEDs start blinking alternately, enter the new code and confirm it with the # key.

7. Using the entry keypad

The INT-SCR multifunction keypad can work in the entry keypad mode (INT-ENT). The main task of the zone keypad is activation of the delay for the 3. INTERIOR DELAYED type zones. The time period during which these zones will act as delayed ones is programmable for the keypad. If more than one zone keypads are assigned to the partition, a different delay unblocking time can be programmed for each of them. After expiry of the programmed time, the interior delayed zones will again operate as instant ones.

7.1 LED indicators

Only the 👁 LED is used. Blinking of the LED indicates that the delay activation time countdown is running (disarming has no effect on the LED blinking).

7.2 Sound signaling

The installer can disable the sound signaling or replace it by blinking of keypad backlight.

During operation, the keypad can generate the following sounds:

1 short beep – pressing any digit key, confirmation that code has been entered or card has been read.

3 short beeps – confirmation of delay activation.

4 short and 1 long beeps – confirmation of the guard round or execution of the control for 24. MONO SWITCH or 25. BI SWITCH type outputs.

3 pairs of short beeps – the user should change his/her code.

2 long beeps – unknown code/card.

3 long beeps – activation the delay is impossible (the partition is disarmed or the delay has already been started) or the function is unavailable.

Additionally, the keypad can audibly signal the DELAY ACTIVATION TIME.

7.3 Functions available from the entry keypad

Depending on the user type and authority level, keypad settings and alarm system status, entering the code and confirming it with the * or # key (presenting the proximity card) will result in:

- activating the delay in partition for 3. INTERIOR DELAYED type zones;
- changing over the status of 25. BI SWITCH type outputs;
- turning on the 24. MONO SWITCH type outputs;
- guard round confirmation.

8. Using the code lock

The basic task of the code lock is to execute the access control function (supervise a single door).

SATEL offers the following code locks:

INT-SZ;

INT-SZK.

The code locks are available with keys backlight in various color versions. The color version is indicated by an additional letter symbol included in the code lock designation (e.g. INT-SZ-GR – green backlight; INT-SZ-BL – blue backlight).

8.1 Description of code locks

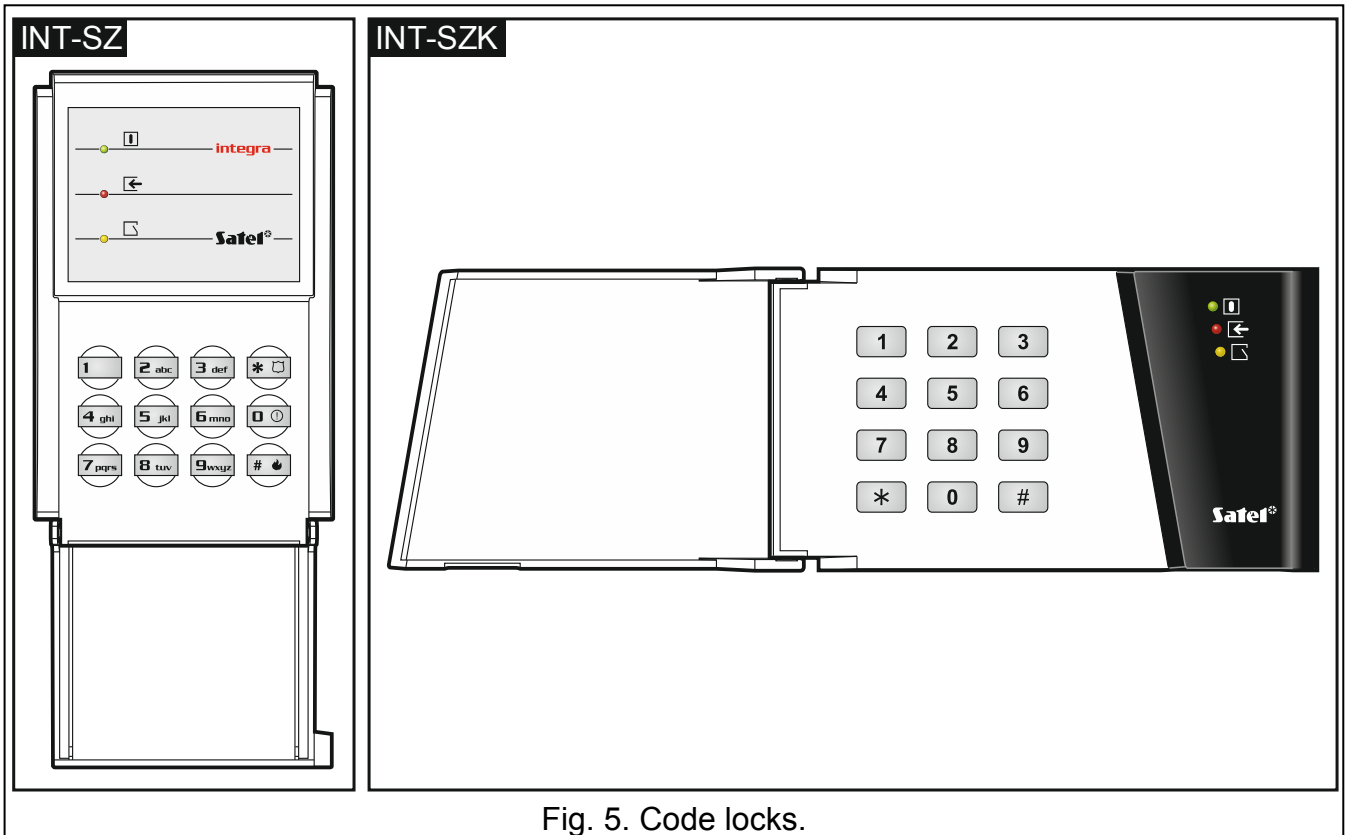


Fig. 5. Code locks.

8.1.1 LED indicators

LED	Color	Function description
	green	**ON** – code lock is operated by the control panel
	red	**ON** – door unlocked
	yellow	**blinking** – door open

Table 5. Description of the code lock LEDs.

All LEDs blinking in turn indicate that there is no communication with the control panel.

8.1.2 Keys

The keys enable user authorization by means of a code and starting of the functions available from the code lock.

8.1.3 Sound signaling

Beeps generated when operating

The installer can disable the sound signaling or replace it by blinking of the keypad backlight.

1 short beep – pressing any digit key or confirmation that code has been entered.

4 short and 1 long beeps – confirmation of door unlocking or execution of another function.

2 long beeps – unknown code/card.

3 long beeps – unavailable function.

Events signaled by sounds

Only installer selected events are signaled.

5 short beeps – zone violation (CHIME).

Very short beeps – door open too long.

8.2 Functions available from code lock

Depending on the user type and authority level, as well as the code lock settings, entering the code and confirming it with the * or # key will result in:

- unlocking the door (activating the relay);
- changing over the status of 25. BI SWITCH type outputs;
- turning on the 24. MONO SWITCH type outputs;
- guard round confirmation;
- enabling temporary partition blocking.

The installer can permit triggering alarms from the keypad. To trigger an alarm, do the following:

fire alarm – press the [# 🔥] (INT-SZ) / [*] (INT-SZK) key for approx. 3 seconds;

medical (auxiliary) alarm – press the 0 key for approx. 3 seconds;

panic alarm – press the [* 🔔] (INT-SZ) / [#] (INT-SZK) key for approx. 3 seconds. The installer defines whether the triggered alarm will be loud (setting off the loud alarm signaling) or silent (without loud signaling).

The installer can permit changing own code by means of the code lock. Proceed in the same way, as when changing the code by means of the partition keypad (see: p. 40).

9. Confirming voice messaging

The installer can configure the control panel so that confirmation of listening to the voice message be required. If there is no confirmation, the control panel can connect many times for playback of the message. Having listened to the message can be confirmed from the keypad of DTMF dialing telephone. The installer defines whether any 4-digit sequence is sufficient to confirm receipt of a voice message, or it must be a specific code. After entering of the code, the control panel will give the following information by means of sound signals:

1 short beep repeated every 3 seconds – the message has been confirmed, wait for playback of the next voice message;

4 short and 1 long beeps – the message has been confirmed, there are no more voice messages;

2 long beeps – an invalid code has been entered (the message has not been confirmed).

If the control panel is sending messages about several events and confirmation of the voice messages is required, each message should be confirmed. The first message must be confirmed before the second message can be played back, an so on.

The installer can configure the control panel so that acknowledgement of receiving the message by the user will:

- *clear messaging other users;*
- *allow to get access to the INT-VG module voice menu.*

10. Call answering and telephone control

The information below does not apply to the control panels to which the INT-VG module is connected.

The call answering and telephone control functions are available to the users who have the **telephone code**. These functions require that the DTMF dialing phone be used. The call answering function allows to get information on the partition status (armed, disarmed). Owing to the telephone control function, it is possible to control the REMOTE SWITCH type outputs using the telephone.

10.1 Answering phone calls

1. Establish connection with the control panel, using one of the following methods (consult the installer to learn which method is supported by the control panel):

   single call – call the telephone number of control panel. The control panel will answer the call after the number of rings programmed by the installer.

   double call – call the telephone number of control panel. Hang up after the number of rings programmed by the installer. Call again within three minutes. The call will be answered by the control panel immediately.

   Establishing connection will be signaled by three short beeps.
2. Enter the telephone code on the telephone keypad. 4 short beeps and 1 long beep will confirm that you have got access to the call answering function. If the entered code is invalid, this will be signaled by the control panel by two long beeps.

If you make a mistake when entering the code, enter the 4 digits anyway, and when the control panel signals that the code is wrong, enter the correct code.

After entering three wrong codes, the control panel will hang up.

In case of a single call, if:

- *no code has been entered and the connection is terminated,*
- *an invalid code has been entered and the connection is terminated,*

the control panel will answer no calls for the next few minutes. It enables e.g. a fax to be connected after the control panel.

3. Within up to 15 seconds, enter the 2-digit partition number (e.g. 01, 07 or 15). The control panel will inform you about the partition status by means of sound signals:
   3 short beeps – partition disarmed;
   4 short and 1 long beeps – partition armed.
   If no key is pressed on the phone for 15 seconds, the control panel will hang up.
4. Upon pressing in turn the 0 and # keys on the telephone keypad, the control panel will hang up.

10.2 Telephone control

1. Get access to the phone call answering function (steps 1-2 in section ANSWERING PHONE CALLS).
2. Within up to 15 seconds, press in turn the 2 and # keys on the telephone keypad. 4 short beeps and 1 long beep will confirm that you have got access to the telephone control function.
3. Within up to 15 seconds, enter the 2-digit number of the remote switch (e.g. 01, 07 or 15). The control panel will inform you about the switch status change by means of sounds:
   3 short beeps – the switch has been turned off;
   4 short and 1 long beeps – the switch has been turned on.

The operating mode of the REMOTE SWITCH type output depends on how the output has been configured by the installer.

4. Upon pressing in turn the 0 and # keys on the telephone keypad, the control panel will hang up. You can also press the 1 and # keys to return to the phone call answering function.

10.3 Audio alarm verification

Remote audio alarm verification is possible when the INT-AV module is connected to the control panel.

1. Get access to the phone call answering function (steps 1-2 in section ANSWERING PHONE CALLS).
2. Within up to 15 seconds, press in turn the 3 and # keys on the telephone keypad. 4 short beeps and 1 long beep will confirm that you have got access to the function of audible alarm verification. The DTMF commands you can use after starting the listen-in / talk session are described in the INT-AV module manual.

11. SMS control only INTEGRA 128-WRL

The INTEGRA 128-WRL control panel can be operated by means of the SMS messages containing suitable control commands. The content of commands and the additional rules of how to use them (using the lower case and upper case letters, adding the telephone code to the content of sent SMS message, etc.) are to be defined by the installer. If appropriate control commands are programmed by the installer, the SMS messages can be used to:

- violate selected zones;
- temporary bypass selected zones;
- unbypass selected zones;
- arm selected partitions in selected mode;
- disarm selected partitions;
- clear alarm in selected partitions;
- activate selected MONO SWITCH type outputs;
- activate selected BI SWITCH type outputs;
- deactivate selected BI SWITCH type outputs;
- toggle selected BI SWITCH type outputs;
- check status of selected partitions;
- send the USSD codes to the operator of SIM card installed in the module (e.g. to check the card account status or recharge it). The answer received from the operator is forwarded in the form of SMS message to the telephone number from which the control command was sent.

When sending the USSD codes, the SMS message must have the following form:

xxxxxx=yyyy=

where "xxxxxx" is the control command and "yyyy" is the USSD code supported by the GSM network operator.

The SMS message may contain several control commands.

If correctly programmed by the installer, the control panel will confirm execution of the control commands by means of SMS messages sent to the telephone number from which the control command was received.

12. Operating the alarm system by means of keyfob

For the INTEGRA 128-WRL control panel or any other control panel to which the ACU-120, ACU-270, ACU-100, ACU-250, INT-RX or INT-RX-S module is connected, you can control the system using the keyfob. The user can have up to 2 keyfobs:

– bidirectional APT-100 keyfob – supported by the ABAX system (INTEGRA 128-WRL control panel, ACU-120, ACU-270, ACU-100 (firmware version 2.00 or newer) or ACU-250 controller);
– 433 MHz keyfob – supported by the INT-RX or INT-RX-S module.

One keyfob enables execution of up to 6 functions. For each keyfob, functions to be executed upon pressing a button / combination of buttons, and for the APT-100 bi-directional keyfobs also information to be displayed on the keyfob LEDs, are individually assigned (see: section ADDING KEYFOB p. 29).

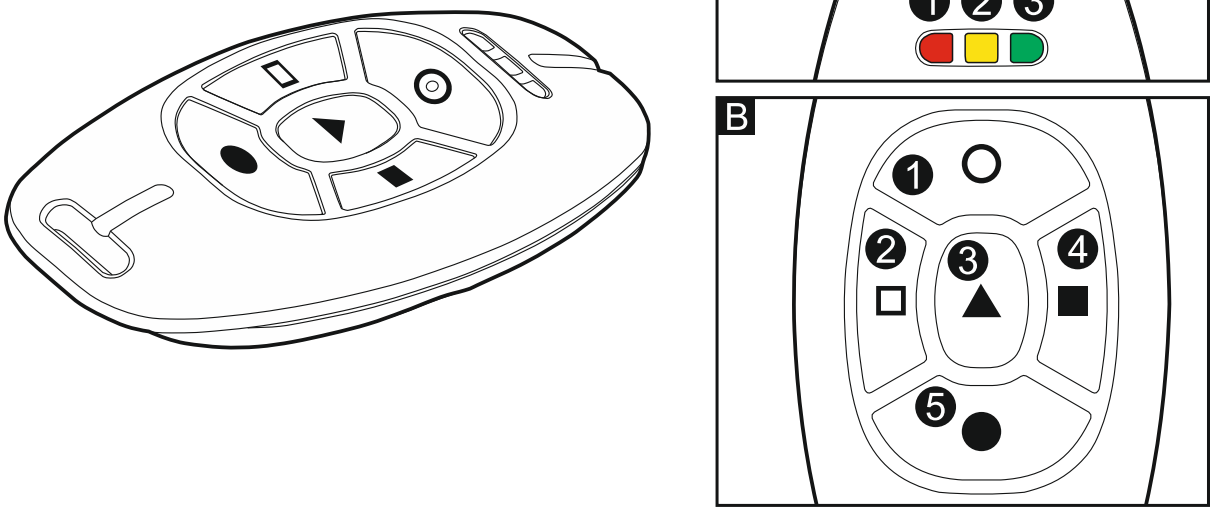


Fig. 6. APT-100 keyfob. A – numeration of LEDs. B – numeration of keyfob buttons.

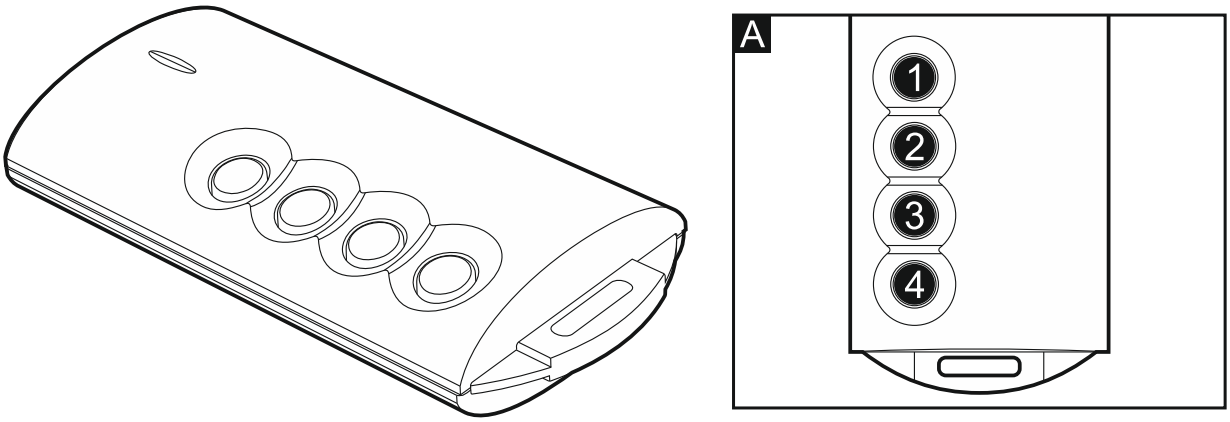


Fig. 7. T-4 keyfob (433 MHz keyfob). A – numeration of keyfob buttons.

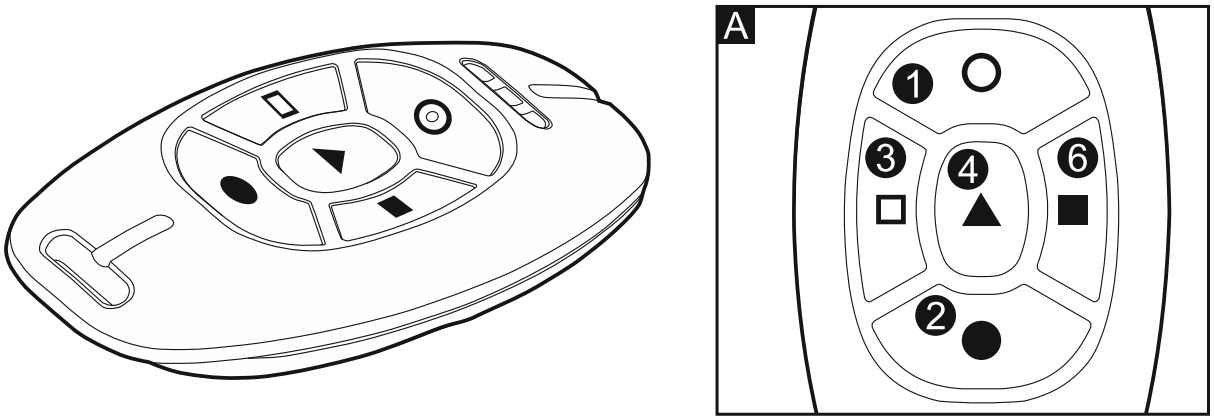


Fig. 8. MPT-300 keyfob (433 MHz keyfob). A – numeration of keyfob buttons. The button designated with digit 6 corresponds to the combination of buttons 1 and 3 in other 433 MHz keyfobs.

13. Manual update history

Date	Firmware version	Introduced changes
2013-08	1.12	• Information on INT-TSG keypad has been added (p. 6). • Note about the user having SIMPLE USER right has been added (p. 10). • List of user functions has been supplemented (p. 11). • Description of CHANGE TELEPHONE CODE user function has been added (p. 18). • Description of SIMPLE USER right has been added (p. 27). • Description of ADMINISTRATOR right has been added (p. 27). • Information on maximum duration of zone testing has been modified (p. 34). • Section "Audio alarm verification" has been added (p. 44).
2013-12	1.12	• Information on the INT-KLFR (p. 5, 6 and 9) and INT-TSI (p. 6) keypads has been added. • Description of IP/MAC ETHM-1 user function has been modified (p. 22).
2014-10	1.13	• Information on the ETHM-1 Plus module has been added. • List of user functions has been supplemented (p. 11). • Note on the possibility to disable user menu shortcuts by the installer has been added (p. 15). • Information on new functionality of the key 0 when editing the multiple-selection list in text mode has been added (p. 16, 23, 31 and 32). • Description of GPRS MONIT.TEST user function has been added (p. 21).

14. Brief description of operating the system from keypad

blinking – trouble or trouble memory / Grade 2: trouble or trouble memory, bypassed zones or alarm

ON – all partitions operated by the keypad are armed
blinking – some partitions are armed

ON or **blinking** – alarm or alarm memory

[CODE]# – arming / disarming / alarm clearing

Quick arming:
0# - full arming
1# - full arming + bypasses
2# - arming without interior
3# - arming without interior and without entry delay

9# – end of exit delay countdown

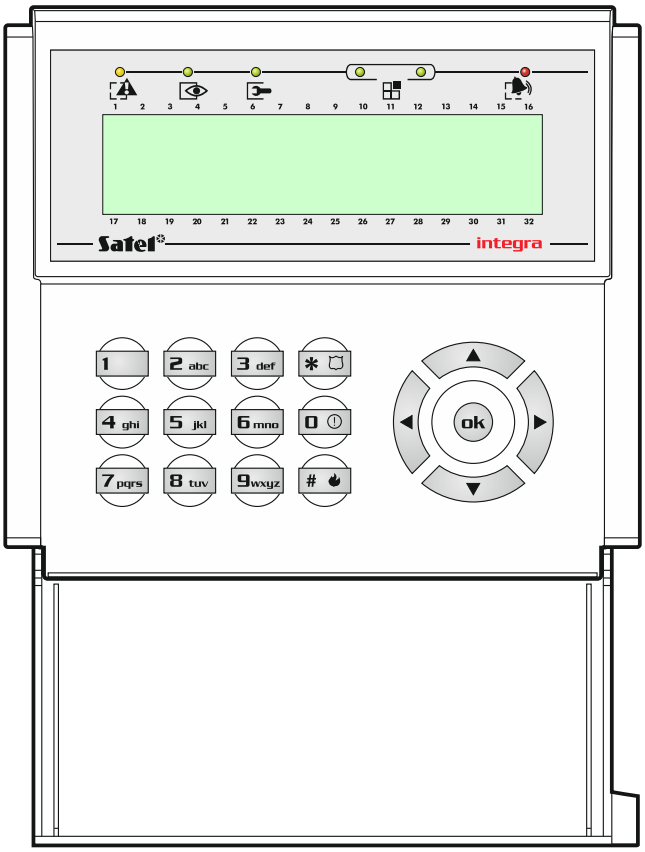
8# – quick control of outputs

[CODE]✱ – enter the user menu
User menu shortcuts:

1	Change own code
2	Users [Masters]
21	New user [New master]
22	Edit user [Edit master]
23	Remove user [Remove master]
4	Zone bypasses
41	Inhibit
42	Isolate
5	Events
51	Selected events
52	All events
6	Set time
7	System state
8	Outputs control
9	Service mode
0	Downloading
01	Start DWNL-RS
02	Finish DWNL-RS
03	Start DWNL-MOD.
04	Start DWNL-TEL
05	Start DWNL-CSD [INTEGRA 128-WRL]
06	Start DWNL-GPRS [INTEGRA 128-WRL]
07	ETHM-1 – DloadX
08	ETHM-1 – GuardX

○ ○ – 1. group (numbers: 1-32 / addresses 00-1F)
○ ● – 2. group (numbers: 33-64 / addresses 20-3F)
● ○ – 3. group (numbers: 65-96)
● ● – 4. group (numbers: 97-128)
(○ – LED OFF; ● – LED ON

blinking – service mode started



Shortcut keys (press for approx. 3 seconds):
1 – check zone status
4 – check partition status
5 – view alarm log
6 – view trouble log
7 – view current troubles
8 – CHIME signal ON/OFF
9 – toggle display between standby mode and partition status mode
ⓘ – trigger medical (aux) alarm
– trigger fire alarm
– trigger panic alarm